UNIVERSIDADE NOVA DE LISBOA
FACULDADE DE DIREITO

Desenvolvimento de um quadro situacional para a cibersegurança em Portugal

Pedro Matos Salvador Vian

Relatório de Mestrado em Direito e Segurança sob a orientação do Professor Doutor Armando Marques Guedes

Lisboa, 2016

Agradecimentos

Vou dedicar este espaço para manifestar a minha gratidão a todos aqueles que, ao longo da realização deste relatório de mestrado, me apoiaram e tornaram possível a sua concretização.

Em primeiro lugar quero agradecer ao Professor Doutor Armando Marques Guedes, orientador desta tese, o apoio e a disponibilidade que demonstrou durante o período de realização deste trabalho.

Agradeço igualmente ao meu co-orientador, Engenheiro José Lino Alves dos Santos, pela generosa oportunidade, de realizar este trabalho com o seu apoio no Centro Nacional de Cibersegurança e pelo seu interesse e no tema.

Em último, mas não menos importante, queria agradecer a toda a equipa do Centro Nacional de Cibersegurança pelo seu apoio até à concretização do trabalho.

Resumo

Hoje em dia, as ameaças são cada vez mais frequentes e sofisticadas, do que alguma vez registado. Todo o tipo de empresas/organizações e informação estão sujeitas a estas ameaças. Estes ataques são cada vez mais recorrentes, deixando para trás um rasto de várias quebras de segurança. Existem uma serie de ciberataques que já deixaram a sua marca na historia. Uma das mais notórias, foi o caso da Estónia em 2007, por um grupo pro-kremlin de Transnístria em que vários servidores governamentais, fornecedores de serviço, servidores da banca, entre outros foram alvo de uma serie de ataques, na sua maioria de DDoS (Distributed Denial of Service[1]),e botnets[2]. O seu método era tao complicado que o governo da Estónia achava que estavam a ser apoiados pelo governo russo. Isto resultou na paragem de um país ate que o problema fosse normalizado. Considerado um ato de hacktivismo[3] pelo que representava algo muito importante para a população russa, um ícone, "the Bronze Soldier of Tallinn", um elaborado cemitério da altura soviética que o governo da Estónia queria recolocar.

Hoje em dia, não só enfrentamos adversários mais sofisticados, como a informação que valorizam é cada vez mais alargada. Estes grupos conseguem

[1] DDoS - Distributed Denial of Service refere-se a uma técnica de sabotagem que assenta no esgotamento dos recursos disponíveis no sistema ou serviço alvo e que resulta na sua degradação ou paralisação. Este esgotamento é conseguido através de um número simultâneo de transações muito superior ao dimensionamento previsto. Estas conexões, indistinguíveis do tráfego legítimo, são normalmente realizadas de forma automática a partir de conjunto de computadores previamente infetados e colo cados sob o comando de um criminoso.

[2] Botnets - Um botnet é uma coleção de programas conectados à Internet que se comunicam com outros programas similares, a fim de executar tarefas. Também é uma coleção de agentes de software ou bots que executam autonomamente e automaticamente. O termo é geralmente associado com o uso de software malicioso, mas também pode se referir a uma rede de computadores, utilizando software de computação distribuída.

[3] Hacktivismo - (uma junção de *hack* e *ativismo*) é normalmente entendido como escrever código fonte, ou até mesmo manipular bits, para promover ideologia política - promovendo expressão política, liberdade de expressão, direitos humanos, ou informação ética. Atos de hacktivismo são carregados da crença de que o uso de código terá efeitos similares aos do ativismo comum ou manifestações civis.

fazer coisas inimagináveis com os bits[4] mais aparentemente inócuos de informações recolhidas. Como tal, é preciso tomar medidas para garantir a segurança dos cidadãos quando navegam no ciberespaço, no qual as fronteiras são desconhecidas, onde a regulação é insuficiente e a segurança é ainda muito precoce.

No plano nacional pode-se afirmar que Portugal possui as capacidades necessárias à proteção do seu ciberespaço. Com a criação do Centro Nacional de Cibersegurança (CNCS), Portugal atingiu um dos objetivos principais da sua estratégia nacional de cibersegurança, em assegurar um ciberespaço livre e seguro e em implementar as medidas e instrumentos necessários à antecipação, deteção, reação e recuperação de situações que, face à iminência ou ocorrência de incidentes ou ciberataques, ponham em causa o funcionamento dos organismos do estado, das infraestruturas críticas e dos interesses nacionais.

Partindo de uma analise à estrutura organizacional da cibersegurança em Portugal este trabalho pretende dar um contributo para o que se considera ser uma necessidade, o desenvolvimento de um quadro situacional para a cibersegurança com o objetivo de melhorar o nível de *awareness* nacional contribuindo assim para o desenvolvimento do modelo de maturidade do CNCS relativamente á prevenção e deteção de incidentes no ciberespaço nacional.

Neste sentido foram formulados um conjunto de estudos com o objetivo de dar a entender ao leitor toda a estrutura de um centro de cibersegurança na qual se destaca a proposta de desenvolvimento de um quadro situacional para a cibersegurança em Portugal.

---

[4] Bits - (simplificação para dígito binário, " ***Bi**nary digi**t*** " em inglês) é a menor unidade de informação que pode ser armazenada ou transmitida, usada na Computação e na Teoria da Informação. Um bit pode assumir somente 2 valores: 0 ou 1, corte ou passagem de energia respetivamente. Embora os computadores tenham instruções (ou comandos) que possam testar e manipular bits, geralmente são idealizados para armazenar instruções em múltiplos de bits, chamados **bytes**. No princípio, byte tinha tamanho variável mas atualmente tem oito bits. Bytes de oito bits também são chamados de **octetos**. Existem também termos para referir-se a múltiplos de bits usando padrões prefixados, como quilobit (**kb**), megabit (**Mb**), gigabit (**Gb**) e Terabit (**Tb**). De notar que a notação para bit utiliza um *"b"* minúsculo, em oposição à notação para **byte** que utiliza um *"B"* maiúsculo (**kB**, **MB**, **GB**, **TB**).

Acrónimos e siglas

AMA - Agência para a Modernização Administrativa

ANS - Autoridade Nacional de Segurança

CEGER - Centro de Gestão da Rede Informática do Governo

CERT - Computer Security Incident Response Team

CNCS – Centro Nacional de Cibersegurança

CNPCE - Conselho Nacional de Planeamento Civil de Emergência

CoE - Conselho da Europa

CPE - Comissão de Planeamento de Emergência

CPEC - Comissão de Planeamento de Emergência das Comunicações

CPECib - Comissão de Planeamento de Emergência do Ciberespaço

CSA – Cyber Situational Awareness

CSIRT - Computer Security Incident Response Team

DDoS - Distributed Denial of Service

DNS - Domain Name System

DoS - Denial of Service

ENISA - European Network and Information Security Agency

FIRST - Forum of Incident Response and Security Teams

GCS - Gabinete Coordenador de Segurança

GNS - Gabinete Nacional de Segurança

GSM - Global System for Mobile Comunications

ICP-ANACOM - Autoridade Nacional de Comunicações

IEC - International Electrotechnical Commission

IETF - Internet Engineering Task Force

IEEE - Institute of Electrical and Electronics Engineers

INA - Instituto Nacional de Administração

IPQ - Instituto Português da Qualidade

ISA - Internet Security Alliance

ISAC - Information Sharing and Analysis Center

ISO - International Organization for Standardization

ISP - Internet Service Provider

ITIJ - Instituto das Tecnologias de Informação na Justiça do Ministério da Justiça

ITU - International Telecommunications Union

NATO - Organização do Tratado do Atlântico Norte

NIST - National Institute of Standards and Technology

OCDE - Organização para a Cooperação e Desenvolvimento Económico

OEA - Organização de Estados Americanos

OCSA – Operational Situational Awareness

PIC - Proteção de Infraestruturas Críticas

PICI - Proteção de Infraestruturas Críticas da Informação

PIX - Portuguese Internet Exchange Point

PJ - Polícia Judiciária

SA – Situational Awareness

SCADA - Supervisory Control And Data Acquisition

SCEE - Sistema de Certificação Eletrónica do Estado

SIRP - Sistema de Informações da República Portuguesa

SSI - Sistema de Segurança Interna

TIC - Tecnologias da Informação e da Comunicação

EU - União Europeia

WARP - Warning, Alert and Reporting Point

Conteúdo

Âmbito, e objetivos do trabalho

As ameaças são reais, e como tal, devem ser desenvolvidas as capacidades necessárias para a proteção do ciberespaço. O fator humano é uma das grandes vulnerabilidades atuais, isto devido ao desconhecimento dos elementos que nos rodeiam, sendo assim importante, a formação e consciencialização de protocolos de segurança e das ameaças presentes.

No inicio deste trabalho, vou abordar um tema relativamente a esta "consciencialização situacional", ou seja, *situational awareness*. Uma organização necessita de um modelo de *situational awareness* para apoiar uma serie de processos críticos para a prevenção e deteção de incidentes e para eliminar o fator humano da sua lista de vulnerabilidades.

Em plena Era da Informação, um dos fatores mais importantes para uma organização é *a* sua base de dados, ou seja, a informação que produz e a que partilha com outras entidades. O tema seguinte que vai ser abordado, diz respeito á importância da informação como medida de prevenção e resposta a ameaças. Para uma segurança eficaz, uma organização tem de possuir a capacidade de produção de informação interna que, após todo o processo de processamento de informação, se transforma em CTI (*cyber threat intelligence*), ou seja, informação que pode ser utilizada para apoiar o processo de tomada de decisão relativamente à resposta a ameaças.

Uma das maiores dificuldades relativamente à cibersegurança é a constante evolução do ambiente virtual, ou seja, todos os dias surgem novas ameaças, o que torna virtualmente impossível estarmos 100% preparados contra todas as ameaças. Esta constante metamorfose do ciberespaço e do espectro de ameaças dificultam bastante as medidas de segurança existentes. Neste capitulo, o ciclo de vida destas ameaças será analisado em pormenor, o que é um ciberataque, e como se processa, serão algumas das questões respondidas, sendo estas respostas cruciais para a compreensão da ameaça e consequentemente para a sua resposta.

A partilha de informação, como vai ser analisada em pormenor neste trabalho, é a palavra chave para o sucesso no desenvolvimento da maturidade de uma organização. Sem uma arquitetura de partilha, uma organização fica limitada pela informação que produz, limitando assim as suas capacidades defensivas. Existem várias arquiteturas de partilha de informação, todas diferentes, mas com o mesmo objetivo final, a partilha de conhecimento entre organizações, que consequentemente contribui para o desenvolvimento de um *situational awareness* dos membros participantes destas comunidades de partilha. Sendo o objetivo deste trabalho contribuir para o desenvolvimento de um quadro situacional para a cibersegurança em Portugal, o foco do mesmo vai incidir nas capacidades estruturais necessárias para um SOC (security operations center) atingir a maturidade necessária para suportar um nível se SA eficaz na resposta a incidentes.

A Internet não é um espaço fora da lei, e é necessário garantir que princípios democráticos, os valores, direitos e liberdades dos cidadãos são cumpridos, sendo que no ultimo capitulo, será analisada a regulamentação existente a nível nacional e o que deve ser revisto para garantir o cumprimento das leis no ciberespaço.

O objetivo deste trabalho é o de apresentar um conjunto de propostas que sirvam como piloto para o desenvolvimento de um quadro situacional para a cibersegurança em Portugal, apresentado ao longo deste trabalho vários estudos realizados no sentido de compreender a estrutura organizacional que seria, ideal para o plano nacional.

Introdução

1. Cyber Situational Awareness, a consciência das ameaças no ciberespaço

No decorrer do século, os avanços tecnológicos provocaram a convergência das telecomunicações e das tecnologias de informação. Isto significou o princípio de uma era conhecida como, Era da Informação. A Era da Informação é caracterizada pelo aparecimento da digitalização, que basicamente implicou a mudança de analógico para digital. Uma característica bastante destinta da Era da Informação é a integração contínua de comunicações informáticas em virtualmente todas as ações do nosso quotidiano e processos críticos que suportam a sociedade moderna, e a tendência de "ligar todo a todos" em que tudo tem de estar conectado. Isto deu origem ao aparecimento da sociedade da informação. No entanto, o aparecimento da sociedade da informação como resultado da integração das tecnologias de informação nas vidas das pessoas também redefiniu assim as noções tradicionais de segurança. A segurança a nível das tecnologias de informação e comunicação tem agora uma influência esmagadora em quase todos os aspetos da sociedade, incluindo na economia global. Assim, com esta revolução na sociedade da informação, práticas maliciosas contra os sistemas de TIC, tais como sistemas de computadores e redes, tem agora o potencial para afetar pessoas, países e a economia global de formas antes inimagináveis. Um dos desafios mais críticos para esta sociedade é prevenção destas ciberameaças para impedir que estas ameaças afetem os seus sistemas, seja por cibercriminosos, hacktivistas ou grupos terroristas. As medidas

utilizadas para responder a estas ameaças vieram a contribuir para a criação do termo “cibersegurança”. A Cibersegurança visa garantir a segurança dos vários utilizadores no ciberespaço. O desafio atual da cibersegurança é maioritariamente para com medidas sociais, legais e tecnológicas de modo a garantir a integridade, confidencialidade, disponibilidade e a segurança geral de toda a informação no ciberespaço de modo a conseguir a confiança dos utilizadores necessária para desenvolver uma sociedade “ciber-consciente”.

Cyber Situational Awareness (CSA) tem atraído muitas atenções, com especial destaque nas estratégias de cibersegurança de vários países. Definir o termo situational awareness é quase tao difícil como o desenvolver e aplicar. Situational Awareness é um fenómeno multifacetado e bem estudado, que pode ser visto de diferentes perspetivas.

O objetivo principal do situational awareness no ciberespaço é o de desenvolver um conhecimento tático e estratégico e que permita ao mesmo tempo responder a ameaças ou tomar decisões de risco. De um ponto de vista técnico, situational awareness resume-se a armazenar, processar, e a filtrar os dados.

O processamento desses dados inclui a necessidade de poder avaliar os fragmentos de dados, assim como informação filtrada e possibilitar uma avaliação da qualidade da mesma. Este por sua vez faz, com que seja possível transformar tecnicamente e avaliar pedaços de dados em informação relevante. Em contraste, o lado cognitivo do situational awareness diz respeito à capacidade humana de ser capaz de compreender as implicações técnicas e chegar a conclusões que levam a decisões informadas. Assim é interessante, cognitivamente, medir ate que ponto um decisor humano está consciente da situação, ex., atingiu um certo nível de situational awareness, e como e que ele(a) vai conseguir manter e desenvolver o seu awareness ao longo do tempo.

A definição mais aplicável e conhecida de situational awareness foi escrita por (Endsley 1988)[5] Pode ser usada como base para essa medição. Esta definição descreve situational awareness cognitivamente como "a perceção dos elementos no ambiente dentro do volume do tempo e espaço, a compreensão dos seus significados e a projeção do seu estado num futuro próximo" Como sugerido por (Endsley 1995)[6], as palavras "perceção", "compreensão", e "projeção" podem ser utilizadas para medir progressivamente o aumento dos níveis de awareness, começando pelo (i) perceção básica de dados importantes, (ii) interpretação e combinação de dados em informação, e (iii) a habilidade de prever futuros eventos e as suas implicações. Estudos mostraram que a habilidade de desenvolver e manter um nível alto de situational awareness varia significamente entre pessoas e tarefas (Endsley 2000). Por necessidade, situational awareness envolve desafios, tanto técnicos, como cognitivos, nos quais os dados base utilizados para o desenvolvimento do awareness consistem num tipo de estimativa subjacente ao estado do mundo, e que, por sua vez, é o resultado do processamento dos dados.

Nas operações de comando e controlo para gestão de crises, planeamento militar, etc, os dados utilizados para desenvolver situational awareness, proveem do resultado da fusão dos dados, ou seja, "O processo de combinar dados para refinar as estimativas e previsões" (Steinberg et al., 1999)[7]

Simplificando, filtragem de dados é o núcleo tecnológico para fundir grandes quantidades de dados em informação compreensível, e um requisito para o desenvolvimento de uma decisão técnica que em ultima analise servirá para

[5] Endsley (1988) = "the perception of the elements in the environment within a volume of time and space, the comprehension of their meaning and the projection of their status in the near future"

[6] Endsley (1995) ="perception", "comprehension", and "projection"

[7] (Steinberg et al., 1999) = "the process of combining data to refine state estimates and predictions"

ajudar o responsável pelo processo de tomada de decisão em causa a ganhar a desenvolver um nível superior de situational awareness.

Assim, no caso do comando e controlo, conclui-se que os lados técnicos e cognitivos do situational awareness estão bastante relacionados, e de alguma forma entrelaçados.

Consideramos assim que "Cyber Situational Awareness é um subconjunto de Situational Awareness, ou seja, Cyber Situational Awareness é a parte de Situational Awareness no ambiente "Cyber", (Amit P.Sheth, 2007). Esse situational awareness pode ser alcançado, por exemplo, pelo uso e dados e sensores de TIC[8] (sistemas de deteção de intrusão, etc.) que podem ser alimentados a um processo de fusão de dados ou serem diretamente interpretados pelo responsável pelo processo de tomada de decisão. Esse nível de situational awareness também pode ser alcançado por sensores mais tradicionais, tais como um "insider informant" a vazar informação sobre um ciberataque eminente. É importante notar que Cyber Situational awareness não pode ser tratada isoladamente, mas está entrelaçada com e é uma parte do situational awareness em si. Embora Cyber Situational Awareness diga respeito a assuntos cyber, esses incidentes cyber tem de ser analisados juntamente com outras informações para se perceber o todo da situação, dai os eventos no ciberespaço oferecem uma visão adicional sobre a situação geral. Na verdade, os acontecimentos no mundo físico oferecem sensores adicionais que fornecem uma visão sobre o ciberespaço. Isto é, a combinação de informação de diferentes áreas abre caminho para uma visão sobre cyber awareness de modo que, por exemplo, a combinação de um sensor virtual (tal como um alarme IDS) e um sensor comum (tal como um

[8] TIC = As **Tecnologias da Informação e Comunicação** é um termo geral que frisa o papel da comunicação (seja por fios, cabos, ou sem fio) na moderna tecnologia da informação. Entende-se que TIC consistem de todos os meios técnicos usados para tratar a informação e auxiliar na comunicação, o que inclui o hardware de computadores, rede, telemóveis, bem como todo software necessário. Em outras palavras, TIC consistem em TI bem como quaisquer formas de transmissão de informações e correspondem a todas as tecnologias que interferem e mediam os processos informacionais e comunicativos dos seres. Ainda, podem ser entendidas como um conjunto de recursos tecnológicos integrados entre si, que proporcionam, por meio das funções de *hardware*, *software* e telecomunicações, a automação e comunicação dos processos de negócios, da pesquisa científica, de ensino e aprendizagem entre outras.

relatório de informações) contribuem para aumentar os níveis de cyber situational awareness.

Pode se dizer assim que cyber situational awareness inclui a perceção de, por exemplo, qualquer tipo de atividade suspeita / interessante que esteja a acontecer no ciberespaço, onde o ciberespaço inclui qualquer tipo de atividade relacionada com redes. Tal atividade suspeita / interessante pode ocorrer a qualquer nível no cachê de TCP/IP e pode variar de uma rede de baixo nível de sniffing para o conteúdo linguístico suspeito num site de social media por exemplo. A atividade de rede detetada fornece uma visão que serve como informação adicional para ser utilizada para obter uma melhor perceção e aumentar os níveis de Cyber situational awareness.

Neste capítulo, cyber situational awareness é analisado de uma perspetiva na qual o situational awareness serve para melhorar o processo de tomada de decisões, tendo em conta que, os novos sensores de rede vão contribuir bastante para o aumento dos níveis de "cyber awareness" com o propósito de se perceber o que tem de ser feito em termos de efeitos desejados e as ações a tomar para atingir esse efeitos (WEICK. 2005). Tendo isto em perspetiva, as infraestruturas de informação com que o cyber situational awareness se aponta podem ser relacionadas em dois contextos distintos, nomeadamente o trabalho de rotina operacional dentro de uma organização (por exemplo, a produção diária), e operações de comando e controlo relacionado com a situação específica (por exemplo, gestão de crises).

Alcançar CSA[9] tem-se provado difícil até a data. No entanto, existem uma serie de problemas que se devem ter em consideração, e que vão permitir um progresso gradual no sentido de alcançar um modelo de CSA que permita a qualquer organização utilizar o seu poder de fornecer informação em tempo real para suportar processos de tomada de decisões e ações proactivas. Esses problemas incluem:

[9] CSA = Cyber Situational Awareness

- Identificação de que decisões e ações a organização possa precisar de tomar em operações Cyber para assegurar que essas operações sejam sustentáveis
- Identificação e acesso aos dados apropriados para suportarem tomada de decisões e ações
- Ferramentas analíticas que permitam a leitura dos dados relacionados com as operações Cyber
- Tecnologia para consolidar e visualizar dados importantes para o processo de tomada de decisão em vários níveis dentro da organização

Modelo Operacional de Cyber Situational Awareness

Quando se obtém o cyber situational awareness necessário para responder ás ameaças presentes é preciso conseguir aplica lo, e, para o fazer é necessário formata lo para um ambiente operacional. Assim, neste capítulo, vou abordar os vários níveis de CSA, que estão repartidos ao longo de uma operação no ciberespaço.

Nível 1

Perceção: *Perception*

A perceção corresponde ao primeiro nível de SA, é através da perceção que temos consciência dos elementos no ambiente que nos rodeia. Em Cyber Situational Awareness a perceção dividi se em duas sub categorias, Deteção e Identificação. A Deteção é responsável por reconhecer eventos e quando se está a dar um ataque ao sistema detetando os mesmos. A Identificação por sua vez é responsável por responder a perguntas como," O que? Quem? Quando? Onde?" de modo a fazer um perfil da ameaça.

Nível 2

Diagnóstico: *Reaction*

O diagnóstico corresponde ao segundo nível de SA, é nesta fase em que as informações sobre as ameaças são recolhidas, analisadas e processadas de modo a criar "Actionable Intelligence", informações relevantes para a resposta as ameaças ao sistema. A fase de diagnóstico e dividida em duas sub categorias, CTI (cyber threat intelligence) e Reação. CTI é uma ferramenta utilizada em cyber para recolha e processamento de informações de forma a criar intelligence que sirva de suporta na resposta a ameaças. Reação é todo o processo de tomada de decisões, análise da ameaça, do impacto, e do alvo de forma a garantir uma resposta rápida e precisa. Este assunto vai ser discutido no capítulo seguinte em maior profundidade.

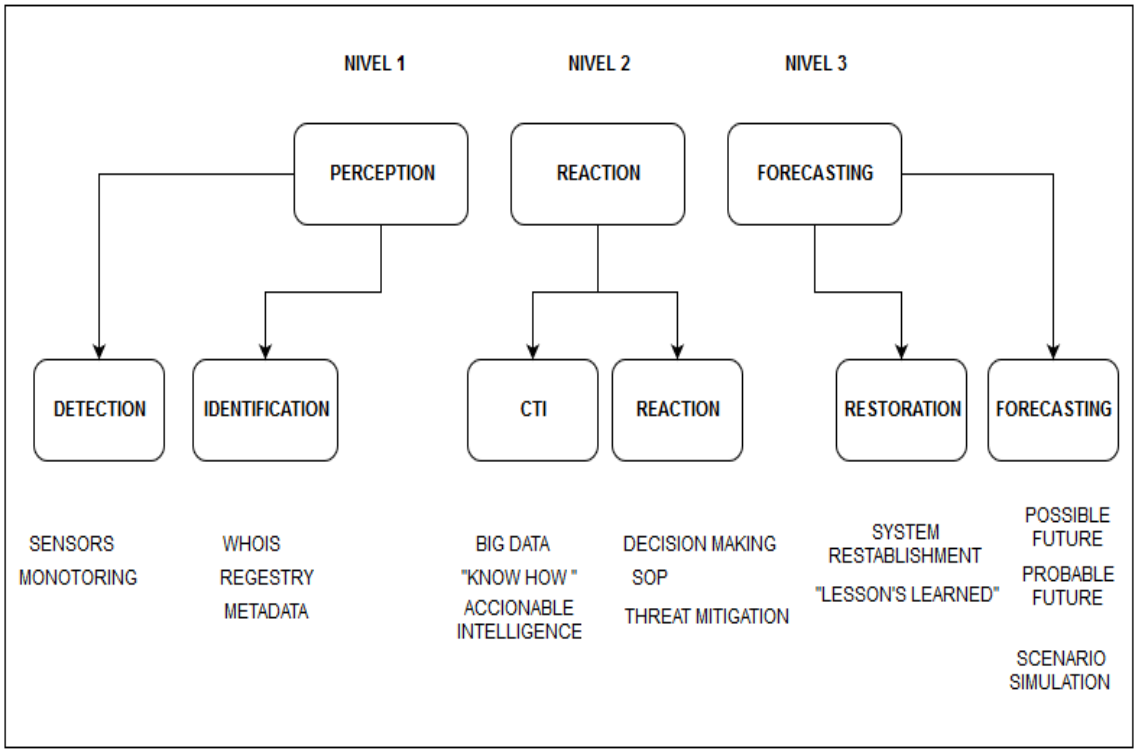
Nível 3

Projeção: *Forecasting*

A projeção corresponde ao terceiro e ultimo nível de situational awareness, nesta

última fase o modelo de segurança tem de ser capaz de desenvolver cenários possíveis de ameaças possíveis e prováveis que possam vir a ocorrer e simula los para que a equipa de resposta a incidentes posso criar mecanismos de defesa contra as mesmas.

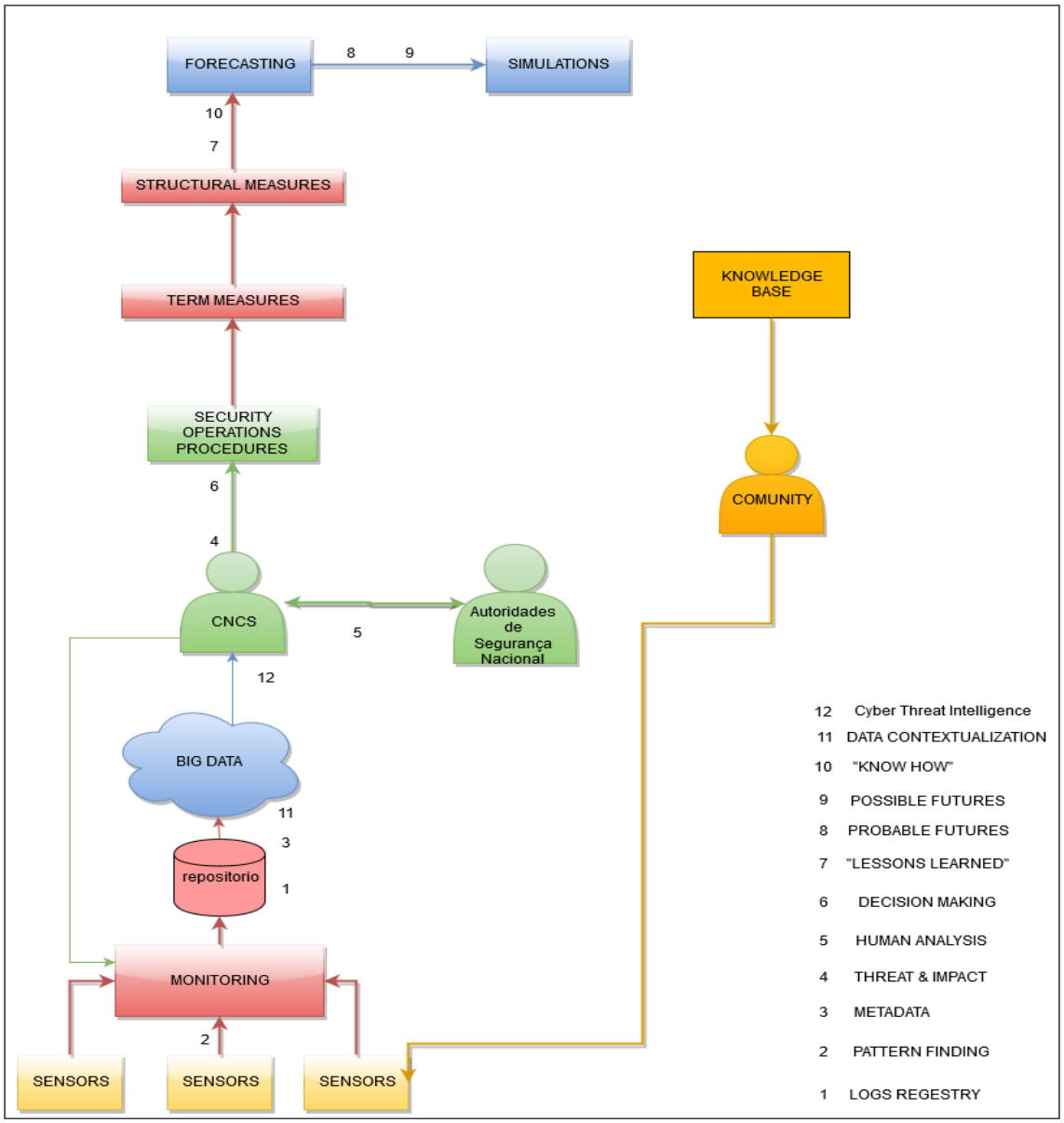
No diagrama abaixo está representado a divisão das várias etapas operacionais de cyber situational awareness; (o diagrama encontra se em inglês devido a termos técnicos que não são traduzíveis)



O diagrama em baixo representa um modelo operacional proposto, desenvolvido neste trabalho. Demonstrando os vários processos e fases da resposta a incidentes no ciberespaço, desde a deteção de anomalias pelos sensores, passando pela monotorização e análise da ameaça, que nos leva ao processo de tomada de decisão.

Como vem representado no diagrama, o processo de tomada de decisão dispõe do contributo e partilha de conhecimento entre várias entidades, que em articulação das suas funções contribuem para a segurança do ciberespaço nacional.

Um modelo de resposta mais maturo vai permitir no futuro a previsão e assim simulação de possíveis incidentes. Estas previsões, são um avanço enorme nas capacidades defensivas de um centro de cibersegurança que vão permitir ao mesmo capacidades de antecipação a ameaças no futuro, evitando assim grandes custos financeiros ás organizações e mesmo ao utilizador comum.



1.1. Analisando o mundo operacional do ciberespaço e o cenário de ameaças

O grande desafio que é enfrentado pela comunidade é a dimensão das bases de dados no ciberespaço (bigdata) e as informações que têm de ser fundidas, analisadas e medidas para formar uma compreensão mais completa sobre as ameaças que as organizações estão a enfrentar. Isto requer, ciência e tradecraft, conhecimento, e uma compreensão de que todas as operações no ciberespaço começam com um ser humano.

O que é um incidente?

Incidentes são grupos discretos de indicadores que afetam uma organização juntamente com informações descobertas ou decidido durante uma investigação de resposta a incidentes. Eles consistem de dados, tais como informações relacionadas com o tempo, as partes envolvidas, ativos afetados, avaliação de impacto, indicadores relacionados, observáveis relacionados, permissões TTP, atores de ameaças atribuídas, efeitos pretendidos, a natureza do compromisso, do Curso de resposta de ações solicitado, Curso de resposta de Ação tomadas, a confiança na caracterização, guia de orientação, fontes de informação de incidentes, o registo das ações tomadas, etc.

O que é um ator de ameaça? (Threat Actor)

Todas as operações no ciberespaço começam com um ser humano. Atores de ameaças são caracterizações dos atores maliciosos (ou adversários) que representam uma ciberameaça, incluindo intenção presumida e comportamento historicamente observados. Num sentido estruturado, atores de ameaças consistem numa caracterização da identidade, suspeita de motivação, suspeita de efeito pretendido.

O que é uma campanha?

Campanhas são grupos de atores de ameaças que perseguem um objetivo, como foi observado através de conjuntos de Incidentes e / ou TTPs, potencialmente entre as organizações. Campanhas são também conhecidas como conjuntos de Intrusion em certas comunidades. Num sentido estruturado, as campanhas podem consistir na suspeita do efeito dos atores de ameaças pretendidos, os TTPs relacionados com permissões dentro da campanha, os incidentes relacionados Acredita-se que parte da Campanha, a atribuição à ator de ameaça acreditava responsável pela campanha, outras campanhas acreditavam estar relacionadas com outro campanha, a confiança na afirmação de intenções agregadas e caracterização da campanha, a atividade feita em resposta à campanha, fonte da informação da campanha, orientação manipulação, etc.

O que são medidas de ação?

COA são medidas especificas ou ações que são tomadas para responder a ameaças, quer sejam corretivas ou preventivas, para responder a exploit targets ou para mitigar potenciais impactos de incidentes. Num sentido estruturado, COA[10] consiste na parte relevante na gestão de ciberameaças.

Níveis de Cyber Threat Intelligence (CTI)

A maioria dos esforços da comunidade de Cibersegurança até a data tem-se focado nas áreas de menos importância como "cyber hygiene", informações tácitas de ciberameaças, e Cyber threat Intelligence tácito. É importante construir uma base e amadurecer á medida que o conhecimento e *tradecraft* de* uma

[10] COA – Courses of action

organização aumenta. Enquanto poucas das organizações hoje em dia se vão focar nos níveis mais altos de Intelligence, é importante perceber em que consistem esses níveis para que os líderes dessas organizações consigam definir estratégias para la chegar.

“Uma boa defesa começa com uma boa estratégia de segurança. Quando tornamos essa estratégia em algo concreto, significa que identificamos e colocamos no sítio certo todas as pessoas, processos e tecnologia necessárias para prosseguir com as operações necessárias para implementar a estratégia, e as ações tácitas especiais para a concretizar. Devido ao foco da comunidade geral, a defesa tem tendência para ter uma visão muito encurtada sobre as ameaças, que é limitada para as ações estratégicas que os atacantes tomam.” (John J. Salerno, 2005). Noutras palavras, temos a tendência a focar-nos no ciclo de vida dos ciberataques ou fases de mitigação que nos fornecem informação tática de cada uma das ameaças como parte de uma operação singular ou ataque. Isto é o foco de Cyber threat intelligence tático e alinha se coma pirâmide de *CTI* *

Cyber Threat Intelligence (CTI) operacional está alinhada com o nível de conhecimento operacional da pirâmide acima. Como tal, CTI operacional produzido a este nível é geralmente baseado em CTI tático durante um determinado período de tempo.

No futuro, os objetivos base para compreender cyber threat intelligence podem ser os referidos abaixo.

O objetivo é desenvolver novos algoritmos que permitam:

a) Melhorar significativamente a “inteligência” das máquinas para ganharem

um awareness próprio para que um dia se protejam sozinhas

b) Automatizar os processos humanos de tomada de decisão e a sua parte cognitiva relativa a processos de awareness.

Se estes objetivos forem bem-sucedidos, os sistemas protegidos vão reconhecer e aprender sobre a evolução das situações, gerar e raciocinar sobre planos de resposta a situação e ações, e responder automaticamente a incidentes.

No capítulo seguinte será abordada uma outra questão, essencial, para a compreensão do *situational awareness* até aqui apresentado. Será feita uma análise completa do que é *cyber threat intelligence*, uma das principais componentes para alimentar os sistemas com informações importantes para distinguir quais são as ameaças reais e as decisões a tomar no que toca a resposta a ameaças.

2. Cyber Threat Intelligence, conhecendo a ameaça

As abordagens tradicionais em cibersegurança que se focam em detetar e compreender vulnerabilidades, fraquezas, e configurações são necessárias, mas insuficientes considerando a dinâmica atual do ciberespaço. Uma defesa eficaz contra ameaças atuais e futuras também requerem um foco externo na compreensão do comportamento, capacidade e intenção do adversário. Só através de uma compreensão equilibrada de ambos o adversário e nós mesmos, é que podemos compreender o suficiente sobre a verdadeira natureza das ameaças que enfrentamos para tomar decisões defensivas eficazes. O desenvolvimento desta compreensão é conhecido como "cyber threat intelligence" (CTI).

"A própria cyber threat intelligence constitui um desafio em que nenhuma organização pode ter informações suficientes para criar e manter o situational awareness necessário do cenário de ameaças" David Waltermire, (2014). Esta limitação é superada através da partilha de informação relevante sobre ciberameaças entre a comunidade e os seus parceiros de confiança. Através da partilha de informações, cada parceiro que participa nesta partilha pode alcançar uma compreensão mais completa do cenário de ameaças que enfrentam e como as mitigar.

"Quando falamos de sistemas de informação, precisamos de ter em conta de que o mais importante é obter informação relevante para dar continuidade ao funcionamento destes sistemas e á sua eficácia. Ou seja, uma ferramenta que nos permita filtrar toda a informação não relevante da que realmente nos interessa, isso é CTI (Cyber Threat Intelligence)." Chris Johnson (2014)

CTI é uma ferramenta que nos permite filtrar a "big data" de modo a obter mos informações relevantes. Para percebermos o que são "informações" é crucial ter

noção de que existe uma grande diferença entre dados e informações[11], e como é que cada um é estruturado.

Threat Intelligence é uma parte vital da resposta a incidentes e segurança de redes. As organizações juntam informações sobre ameaças ativas nos seus sistemas e implementam medidas de segurança. Threat intelligence inclui informação sobre ameaças, TTP's, e outros dispositivos que os atacantes utilizem; os sistemas e informações em que eles se focam; e qualquer outro tipo de informações relacionadas com ameaças que providenciem um aumento no situational awareness dos analistas responsáveis pela segurança da rede e resposta a incidentes. Threat intelligence eficaz demonstra as seguintes características:

- Oportunas – As informações devem ser rapidamente entregues (ex. idealmente a velocidade da rede), com o mínimo de interrupções possível e que forneça oportunidades suficientes para o recipiente se antecipar á ameaça e preparar uma resposta capaz. A relevância da informação está dependente do contexto e tem de ter em conta a volatilidade da ameaça, a velocidade do ataque, e a capacidade e TTP's do atacante. Alguns processos de decisão podem requerer que a informação tática seja entre entregue em segundos ou minutos para responder a um atacante que seja muito rápido, outras ameaças podem ser mais lentas e podem ser respondidas e analisadas com tempo utilizando assim informações mais trabalhadas.

- Relevantes – Threat Intelligence deveria ser aplicável dentro do sistema operativo alvo, identificando as ameaças que essa organização poderia vir

[11] Data and information are interrelated. Data usually refers to raw data, or unprocessed data. It is the basic form of data, data that hasn't been analyzed or processed in any manner. Once the data is analyzed, it is considered as information. Information is "knowledge communicated or received concerning a particular fact or circumstance." Information is a sequence of symbols that can be interpreted as a message. It provides knowledge or insight about a certain matter.

a enfrentar, que tipo de ataques que poderiam vir a sofrer, e descrever quem seriam os atacantes que os poderiam vir a ameaçar. Threat Intelligence neste sentido deveria realizar uma análise de risco para determinar o nível de risco associado a uma ameaça em particular.

- Precisas – Threat Intelligence deve ser correta, completa e inequívoca. Informação imprecisa ou incompleta pode causar a tomada de ações desnecessárias, resultar em respostas inapropriadas.

- Especificas – Threat intelligence deve descrever o incidente ou atacante com um nível de detalhe que correspondam á ameaça com o máximo rigor possível, e que permita perceber se o impacto que a ameaça teria no sistema, para permitir uma avaliação de medidas de ação possíveis.

- Utilizáveis – Threat Intelligence devia, idealmente, identificar medidas que possam ser tomadas para combater as ameaças ou fornecer informação suficiente e contexto que permita o desenvolvimento de uma resposta eficaz para a ameaça em causa.

As organizações não devem apenas partilhar informação sobre intrusões de sucesso, mas também sobre tentativas de intrusão, independentemente de a intrusão ter tido ou não sucesso. Fontes de informação incluem darknet servers[12]

[12] Darknet servers - Uma ***darknet*** é qualquer rede fechada, contendo um grupo privado de pessoas com o intuito de se comunicar. Entretanto, desde 2002, o termo evoluiu e tem sido usado para se referir às redes de compartilhamento de arquivos, sejam elas privadas ou acessíveis ao público em geral. O termo ***Dark Web*** é usado para se referir coletivamente a todas redes secretas de comunicação. De uma maneira geral, uma *darknet* é um grupo que permite compartilhar todo tipo de conteúdo de maneira anônima, sendo impossível identificar o usuário, e também privativa pois os arquivos disponibilizados são criptografados. As *darknets* são utilizadas, portanto, para compartilhar informações sigilosas. A darknet está associada à "deepweb" onde como referido anteriormente o seu IP é redirecionado para outro IP fora do país, é assim um servidor fantasma. WASTE , Freenet são duas das mais conhecidas *darknets*, sendo que esta última suporta até milhões de usuários compartilhando conteúdo.

(ex. servidores configurados para captura de trafego destinado a endereços de IP's não alocados), firewalls, e logs de IDS/IPS. Relatórios sobre tentativas de intrusão geralmente requerem uma análise menor, e podem ser geralmente partilhados e respondidos assim mais rápido.

Existem varias fontes para CTI (cyber threat intelligence), as organizações podem coletar e desenvolver intelligence internamente ou adquiri la externamente através de comunidades de partilha, fontes abertas, parcerias, fontes em setores industriais, vendedores de produtos, serviços comerciais de Cyber threat intelligence, clientes, forças policiais, ou outras entidades de resposta a incidentes.

Quaisquer informações sobre os motivos e objetivos do atacante são extremamente valiosos e deveriam ser documentados. Relações pessoais com indivíduos de confiança ou organizações são excelentes fontes de informação, com a ressalva de que as relações informais podem não ser fonte de threat intelligence duradoura tendo em conta que certos indivíduos podem mudar de organização ou assumirem uma posição diferente dentro da sua organização que já não lhes permita ter acesso á informação previamente partilhada. Fontes internas de threat intelligence incluem sistemas de deteção e proteção de intrusões, produtos de segurança de informação e gestão de eventos, software antivírus e software de alertas de verificação de integridade de ficheiros; sistemas operativos, rede, serviços, e logs de aplicações[13]. A threat intelligence interna e artefactos relacionados que são colecionados devem ser retidos e partilhados com as organizações parceiras tal como é permitido pelas políticas organizacionais.

Threat Intelligence também pode ser adquirido através de comunidades de partilha organizadas pelos sectores da indústria como, finanças, eletricidade ou saúde. As organizações que funcionam dentro de um sector específico deveriam considerar juntar-se a uma comunidade de partilha estabelecida ou, se esta não existir, considerar formar uma com outro par sectorial. As organizações que

[13] NIST SP 800-61 - Computer Security Incident Handling Guide, Section 3.2.3, for additional information on common sources of precursors and indicators

operam no mesmo sector tem, normalmente, missões semelhantes ambientes operacionais semelhantes, e enfrentam frequentemente as mesmas ameaças. Para além destes grupos do sector industrial, existem outras comunidades que ajudam as forças de segurança, entidades governamentais, equipas de emergência, e outros afiliados.

Existem muitas fontes abertas de threat intelligence, acessíveis pela internet, que publicam indicadores de compromisso, blacklists[14], informação sobre vírus e malware, listas de spams[15], e outras informações relativamente a ameaças inerentes. A informação recolhida destas fontes pode ter de ser selecionada manualmente e analisada; um processo demorado, trabalhoso, e com grande possibilidade de cometer erros. As organizações que não são capazes ou não querem ter o trabalho podem considerar a utilização de serviços comerciais de cyber threat que forneçam threat intelligence semelhante e outros serviços uteis por um preço.

[14] Blacklists- In computing, a **blacklist** or **block list** is a basic access control mechanism that allows through all elements (email addresses, users, URLs, etc.), except those explicitly mentioned. Those items on the list are denied access. The opposite is a whitelist, which means only items on the list are let through whatever gate is being used. A greylist contains items that are temporarily blocked (or temporarily allowed) until an additional step is performed. For example, a company might prevent a list of software from running on its network or a school might prevent a list of web sites from being accesses on its computers.

[15] Spam- O termo ***spam*** pode significar Sending and Posting Advertisement in Mass, ou "enviar e postar publicidade em massa", ou também: **S**tupid **P**ointless **A**nnoying **M**essages que significa mensagem rídicula, sem propósito, e irritante. No entanto, existem diversas versões a respeito da origem da palavra *spam*. A versão mais aceita, e endossada pela RFC 2635, afirma que o termo originou-se da marca SPAM, um tipo de carne suína enlatada da Hormel Foods Corporation, e foi associado ao envio de mensagens não-solicitadas devido a um quadro do grupo de humoristas ingleses Monty Python. Na sua forma mais popular, um *spam* consiste numa mensagem de correio eletrônico com fins publicitários. O termo *spam*, no entanto, pode ser aplicado a mensagens enviadas por outros meios e em outras situações até modestas. Geralmente os *spams* têm caráter apelativo e na maioria das vezes são incômodos e inconvenientes.

2.1. Como obter Cyber Threat Intelligence:

A ideia por trás de Cyber Threat Intelligence (CTI) é a de fornecer a capacidade de reconhecer e agir sobre indicadores de cenários de ataque e de compromisso em tempo hábil.

“Enquanto bits de informação sobre ataques abundam, intelligence sobre ciberameaças reconhecem os indicadores de ataques à medida que estes progridem, em essência, o que faz é colocar essas peças em conjunto com o conhecimento compartilhado sobre os métodos e processos de ataque.” (Shawn Riley, 2015)

A campanha envolvida num cenário de ameaça avançado pode levar-nos a fazer perguntas como: "Quem está nos está a atacar?" "Que métodos é que eles estão a utilizar" e "Quais são os sistemas que estão a atacar?" Compreender o que queremos saber sobre os atores das ameaças e os seus métodos, e como prevenir ou detetar ataques, pode ser uma grande ajuda para acelerar o processo de tomada de decisão e as ações a tempo para mitigar as ameaças.

2.2. Actionable Cyber Threat Intelligence

“O Cenário de ameaças hoje em dia requer múltiplas fontes de CTI que sejam autonomizadas para que tenham alguma relevância na resposta a incidentes. A capacidade mais importante de resposta a incidentes é a de fazer perguntas sobre o ambiente do ciberespaço nos quais as ameaças estão em constante transformação.” (Mathew Varghese, 2014)

Enquanto a guerra do cibercrime continua a evoluir, os criadores de malware e os desenvolvedores de exploits estão a elevar cada vez mais o seu nível de sofisticação. Para alguns alvos importantes, as ciberameaças vão desenvolver variantes de malware e morphing code para contornar os controlos de segurança tradicionais, como a assinatura à base de sistemas de deteção de intrusão IDSs e Firewalls[16]. Estes avanços na compreensão das técnicas e ferramentas utilizadas pelos atacantes são essenciais para a compreensão de várias ameaças avançadas de hoje. A rápida comunicação de informações sobre as ameaças tem avançado com o estabelecimento de indicadores mais sofisticados, com base em padrões de compromisso (CPI) que encapsulam descrições ricas das ameaças e incorporam lógicas e / ou condições entre assinaturas tradicionais, tais como nomes de arquivos, entradas de registo e processos em execução.

[16] Firewall é uma solução de segurança baseada em hardware ou software que, a partir de um conjunto de regras ou instruções, analisa o tráfego de rede para determinar quais operações de transmissão ou receção de dados podem ser executadas. "Parede de fogo", a tradução literal do nome, já deixa claro que o firewall se enquadra em uma espécie de barreira de defesa. O objetivo de um Firewall é bloquear tráfego de dados indesejado e liberar acessos bem-vindos.
Um firewall pode impedir uma série de ações maliciosas: um malware que utiliza determinada porta para se instalar em um computador sem consentimento do usuário, um programa que envia dados sigilosos para a internet, ou uma tentativa de acesso à rede a partir de computadores externos não autorizados, por exemplo.

2.3. Tipologias de Cyber Threat Intelligence

Informações sobre ameaças isoladas:

Apesar destes avanços, ainda há muitos desafios com o estado atual da ecosfera de threat intelligence, embora o aparecimento de padrões para *IOCs*[17] *(por exemplo STIX, Yara, OpenIOC)* que produzem máquinas que permitem a sua filtragem, as empresas não têm o apoio das suas ferramentas de segurança para aceder ao verdadeiro conteúdo de threat intelligence.

Muitas vezes a melhor informação permanece isolada, enquanto ataques potencialmente evitáveis continuam a afetar o sistema. E quando se poderia integrar feeds de cyber threat intelligence com ferramentas como, SIEM[18], IDS, ou firewall, estes normalmente continuam isolados a partir dos seus processos de segurança end-to-end.

[17] IOCs - **Input/Output Control System (IOCS)** is any of several packages on early IBM entry-level and mainframe computers that provided low level access to records on peripheral equipment. IOCS provides functionality similar to **File Control Processor** (FCP) in RCA 3301 Realcom Operating System and **GEFRC** in GECOS. Computers in the 1950s and 1960s typically dealt with data that were organized into records either by the nature of the media, e.g., lines of print, or by application requirements. IOCS was intended to allow Assembler language programmers to read and write records without having to worry about the details of the various devices or the blocking of logical records into physical records. IOCS provided the I/O support for several compilers.

[18] SIEM - Do Inglês SIEM (Security Information and Event Management) é uma solução de Software que combina SIM (Security information management) e SEM (Security event manager). Uma solução SIEM permite que os eventos gerados por diversas aplicações de segurança (tais como firewalls, proxies, sistemas de prevenção a intrusão (IPS) e antivírus sejam coletados, normalizados, armazenados e correlacionados; o que possibilita uma rápida identificação e resposta aos incidentes. Enquanto ferramentas SEM oferecem monitoramento em tempo real dos eventos de segurança, coletando e agregando os dados (com resposta automática em alguns casos); uma ferramenta SIM oferece análise histórica dos eventos de segurança, também coletando e correlacionando os eventos, porém não em tempo real; o que permite consultas mais complexas ao repositório.

Disparidade de dados:

Apesar do aparecimento de padrões para IOCs, de threat intelligence que se acumula em diversos formatos, não estruturados, tais como alertas de Siems, IDSs ou e-mails que devem ser vasculhados cuidadosamente, priorizados e traduzidos em cyber threat intelligence utilizável. Sem padrões para medir a qualidade, relevância ou credibilidade das fontes de informação, é complicado priorizar as ações. Organizações que utilizam múltiplas fontes frequentemente deparam se com dificuldades e com uma relação sinal-ruído, que é alta demais para ser de qualquer valor, ou seja, desmaiada informação para ser analisada.

O cenário de ciberameaças atual exige múltiplas fontes de informação automatizadas sobre estas ameaças, a fim de ter valor real para a resposta a incidentes.

Falta de automatização:

O volume de informações sobre ameaças e a taxa a que os feeds são atualizados torna quase impossível para os profissionais de segurança de a acompanharem. E quando ocorre um incidente, a atenção é focada na tática da resposta, recuperação e investigação. O cenário de ameaças atual exige múltiplas fontes de informação sobre ameaças automatizadas, para possuírem qualquer valor real para a resposta ao incidente.

O que queremos dizer por integrada, automatizada e acionável?

Integrado – informações sobre ameaças devem ser integradas de forma holística em todo o seu processo de resposta a incidentes e do conjunto de ferramentas em geral. O conteúdo de threat intelligence deve ser integrado nas suas ferramentas de segurança, como a IDS, Firewall, SIEM, e AV, mas também nos seus sistemas de infira-estrutura de gestão, tais como gestão de patches, gestão de configuração

e recuperação de software acelera quando não se tem que parar para mudar de ferramentas.

Automatizados - para caça de indicadores de compromisso (IOCs) contra o ambiente existente (plataformas, aplicações, dispositivos e outras variáveis) fornecem a velocidade que se precisa para uma caça eficaz e uma vez que as medidas de ação são descobertas, é essencial implementar táticas de remediação em grande escala. A capacidade mais importante para a resposta ao incidente é perguntar qualquer questão do meio ambiente, porque as ameaças estão constantemente a mudar de cor e a área de superfície de ataque vai se alternando ao mesmo tempo.

Acionável - O objetivo é ver o conteúdo de threat intelligence que é relevante apenas para os dispositivos, aplicações e plataformas que estão na rede se não é relevante, não é recorrível. Além da relevância, o conteúdo threat intelligence deve fornecer informações suficientes para torná-lo acionável. Mas não termina aí, nas redes corporativas complexas de hoje, não é só o conhecimento que importa, mas também gestão. Prosseguir uma estratégia de Cyber threat intelligence que permita um caminho para executar táticas defensivas, como deteção automática e correção, e não apenas de pesquisa de segurança para proveito próprio.

Neste capitulo percebemos o que é cyber threat intelligence, para que serve, e como deve ser utilizada para melhorar o nível de segurança de uma organização ou mesmo partilhar com outras entidades contribuído assim para a melhoria da relação e cooperação entre organizações. No capitulo seguinte serão apresentadas respostas as seguintes perguntas relativamente ao mundo das ciberameaças: como começam? Como se processam? E por fim como as podemos evitar? Apresentado um conjunto de fatores resultantes da minha pesquisa que permitem compreender todo o processo de um ataque, desde a sua criação ate ser concretizado, das suas falhas, e como estas podem ser exploradas.

3. O ciclo de vida de um ciberataque

As estratégias de ataque também evoluíram, ao invés de um ataque tradicionalmente direto contra um servidor ou ativo, as estratégias hoje em dia envolvem múltiplos processos, mais pacientes, que incluem exploits e malware, organizando um ataque á rede coordenado, tornando os muito mais perigosos.

Como exemplo, um ataque geralmente começa por simplesmente atrair uma pessoa a clicar num link infetado. A página para o qual se é redirecionado explora remotamente o usuário, e ganha acesso ao computador do utilizador sem este se aperceber. O malware assim instalado no computador da pessoa funciona como um ponto dentro da rede, permitindo ao atacante expandir a dimensão do seu atacante procurando outros ativos dentro dessa rede interna, escalando os privilégios dentro da máquina infetada.

A grande vantagem de o malware e os exploits de rede ao invés de separados como antigamente, é de que agora estão integrados no processo decorrente. Para além disso, o malware ou um exploit não são por si só um fim, mas simplesmente percussores para o próximo passo de um plano de ataque mais complexo.

O Malware, que é cada vez mais sofisticado para evitar deteção, oferece ao atacante acesso remoto, um mecanismo de persistência, e a rede permite ao malware que se adapte e interaja com o ambiente que infetou. Os componentes chave destas estratégias avançadas de ataque incluem, infeções, persistência, comunicação, e comando e controlo.

“Para se compreender Cyber Threat Intelligence (CTI), é necessário primeiro compreender o ciclo de uma ameaça. Os ataques realizados por adversários estão a crescer em grande escala, complexidade e frequência. Estratégias reativas de defesa não são as adequadas para lidar com ameaças persistentes avançadas que

utilizam ferramentas sofisticadas, zero-day exploits[19], e malware[20] avançado para comprometer sistemas e redes." (Seclab, 2015)

Enquanto a gestão de vulnerabilidades e configuração de sistemas continuam a ter um papel importante nas estratégias de defesa das organizações, estes métodos não conseguem responder a 100% às ameaças existentes, com ataques que utilizam técnicas avançadas de intrusão. Embora não seja possível prever totalmente o comportamento adversário, o modelo de um ciclo de vida de um ciberataque pode fornecer uma simples, mas útil abstração do cenário para analisar ameaças potenciais. Cada fase no ciclo de vida de um ciberataque é uma oportunidade para alguém que esteja a proteger uma rede, reagir a uma ameaça. Ao se utilizar o ciclo de vida de um ciberataque, em conjunto com ambas as informações de ameaças internas e externas, os analistas podem desenhar estratégias proactivas de resposta a incidentes que se focam em mitigar as ameaças no princípio do seu ciclo de vida (ex. antes do exploits acontecer).

Existem varias fases no ciclo de vida de um ciberataque[21], como referido abaixo.[22]

---

[19] Zero-day Exploits - Um ataque de exploração de dia zero (ZETA) ocorre no mesmo dia em que é descoberto um ponto fraco num software. Nesse momento, é explorado antes de o criador disponibilizar uma correção. Inicialmente, quando um utilizador descobre um risco de segurança num programa, pode comunicá-lo à empresa de software que, por sua vez, irá desenvolver um patch de segurança para corrigir a falha. O mesmo utilizador pode também divulgar a falha na Internet, alertando outros utilizadores. Normalmente, os criadores de programas criam rapidamente uma correção que melhore a proteção do programa mas, por vezes, os piratas têm conhecimento da falha antes e exploram-na rapidamente. Quando isto acontece, existe pouca proteção contra um ataque uma vez que a falha no software é tão recente.

[20] Malware - O "***malware***", termo do inglês "***malicious software***", é um *software* destinado a infiltrar-se em um sistema de computador alheio de forma ilícita, com o intuito de causar alguns danos, alterações ou roubo de informações (confidenciais ou não). Ele pode aparecer na forma de código executável, scripts de conteúdo ativo, e outros softwares. "*Malware*" é um termo geral utilizado para se referir a uma variedade de formas de *software* hostil ou intruso. O termo *badwares* é às vezes utilizado e confundido com *softwares* prejudiciais não intencionais. *Malware* inclui vírus, worms, cavalos de tróia, ransomware, spyware, adware e outros programas maliciosos. A partir de 2011, a maioria das ameaças de *malware* ativos foram *worms* ou cavalos de troia, em vez de vírus. Desse modo, o *malware* é conhecido como contaminante de computador, como nos códigos legais de vários estados estadunidenses. *Malware* é muitas vezes disfarçado, ou encaixado dentro de arquivos não maliciosos.

[21] Cyber Kill Chain: a life cicle of a cyber attack of Lockheed Martin

[22] The attack phase steps presented in NIST SP 800-115, Technical Guide toInformation Security Testing and Assessment: A Security Life Cycle Approach are presented in the context of a penetration testing activity, but the activities described are similar to those that would be performed by an actual adversary"

- Fase 1 - Reconhecimento: O atacante identifica e escolhe o alvo
- Fase 2 – Preparação: O atacante carrega um exploits dentro de um programa desenhado para executar no computador/rede alvo
- Fase 3 – Transporte: O atacante faz chegar o malware ao sistema alvo
- Fase 4 - Exploração: O atacante executa o seu código no sistema alvo
- Fase 5 – Instalação: O atacante instala software de acesso remoto que fornece uma presença persistente no sistema do alvo.
- Fase 6 – Comando e controlo: O atacante aplica mecanismos de acesso remoto para estabelecer um canal de comando e controlo com o aparelho comprometido
- Fase 7 – Concretização dos objetivos: O atacante alcança os seus objetivos pretendidos (ex. roubo de dados)

Em cima foram referidas as fases de vida de um ciberataque, do ponto de vista da ameaça, em baixo vou referir as fases de mitigação de um ciberataque, mais conhecida como "cyber kill chain"

3.1. Cyber Kill Chain:

Reconhecimento – Monitorizar e analisar o Netflow, darknet, e passive DNS data para detetar e investigar padrões comuns de reconhecimento tais como scans de portas ou sondas. Introduzir medidas de anti reconhecimento tais como redirecionar um atacante para uma rede armadilhada ou bloqueando um adereço de IP especifico ou domínio.

Preparação – Desenvolver, introduzir, e refinar as assinaturas de alta fiabilidade baseadas na análise de artefactos observados em malware payloads. Métodos de

deteção baseados em assinaturas são geralmente frágeis; os atacantes podem evitar deteção através de modificações nos exploits. Ao se realizar uma análise em profundidade dos artefactos com malware capturados, podem ser criadas assinaturas de deteção mais precisas e duradouras, e técnicas adicionais podem ser selecionadas e utilizadas, para identificar novos malware e variáveis de malware existentes.

Intrusão - Perceber as técnicas e ferramentas que o atacante utiliza para infiltrar o malware no sistema, e desenvolver medidas de deteção e prevenção para quebrar os canais de distribuição dos atacantes. Estas medidas podem ser técnicas (ex. blacklisting[23] de um site associado com um ataque de "watering hole"[24])

Exploits – Prevenir tentativas zero-day ao montar defesas que ajudem a prevenir os atacantes de injetarem código malicioso num programa a correr, explorando condições vulneráveis, injetando comandos no sistema operativo, ou usando vulnerabilidades nos controlos de acesso para ganhar acesso total ao sistema.

Instalação – Expor e responder ao malware recentemente instalado ao colocar assinaturas de deteção de intrusão no administrador e na rede e ferramentas de verificação de integridade de ficheiros, deteção de rootkit[25] e monotorização de alterações na configuração do sistema.

Comando e Controlo – Estabelecer bases para o funcionamento normal da atividade entre a rede e dispositivos e configurar a rede interna para detetar anomalias no trafego de rede que entra e sai e em alterações nos comportamentos dos usuários e dispositivos. A monitorização de fugas ao padrão permite a

[23] Blacklisting - Blacklist trata-se de uma lista de e-mails, domínios ou endereços IP, reconhecidos como fontes de spam. Geralmente, utiliza-se este recurso (blacklist) para bloquear os e-mails suspeitos de serem spam, no servidor de e-mails. Em alguns casos, os filtros configurados no programa leitor de e-mails também podem utilizar blacklists.

[24] Watering Hole – O termo "Watering Hole" refere-se á iniciação de um ataque contra empresas ou organizações alvo. Num cenário de ataque "watering hole" , os atacantes comprometem cuidadosamente um website selecionado ao inserirem um exploit que vai depois infetar a maquina com malware

[25] Rootkit – É um tipo de software, muitas das vezes malicioso, projetado para esconder a existência de certos processos ou programas de métodos normais de deteção e permitir contínuo acesso privilegiado a um computador.

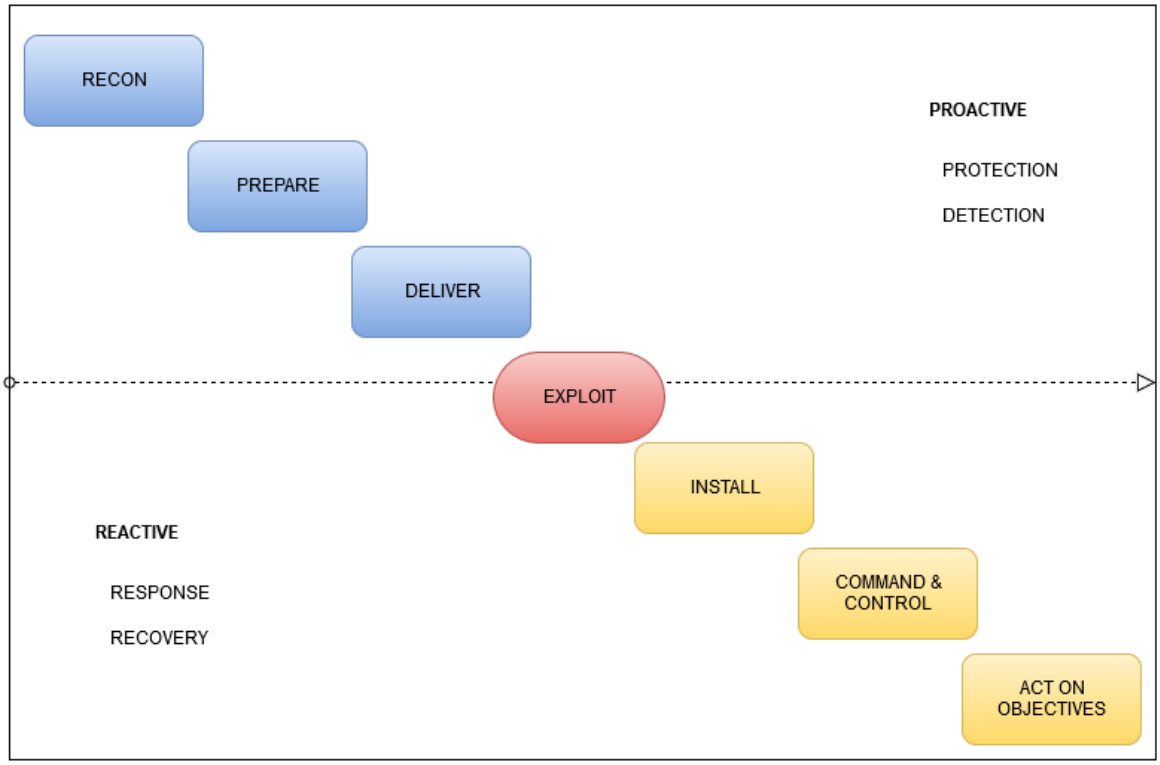
deteção de beaconing (ex. trafego externo á rede em intervalos regulares) que possam estar associados com interações com um servidor de comando e controlo.

Concretização de Objetivos – Aplicar soluções avançadas para a prevenção da perda de dados para detetar acessos anormais a dados, técnicas de evasão, e tentativas de roubo de informação para prevenir transmissões não autorizadas ou cópias de informações sensíveis.

Para se montar uma defesa ativa, uma organização deve procurar compreender o TTP[26] do atacante dentro do ciclo de vida de um ciberataque, possuir e utilizar as informações detalhadas sobre ameaças que sejam relevantes. A partilha de informações entre organizações é um método eficaz para se desenvolver este nível de awareness. Ao se observar os alvos de um atacante, as suas atividades, e comportamentos durante um longo período de tempo, um conjunto de TTP's podem ser desenvolvidos para esse atacante. Partilhar esta informação com outras entidades na área da defesa vai permitir que os mesmos adquiram uma visão mais precisa das estratégias dos atacantes e dos seus planos em geral, assim aumentando a capacidade de antecipação relativamente a intrusões e desenvolvendo assim um situational awareness mais eficaz melhorando o nível de segurança em geral.

[26] TTP - TTP +é um termo militar que significa "táticas, técnicas, e procedimentos"

Na figura abaixo está representado um diagrama desenvolvido neste trabalho que pretende representar graficamente os vários processos de um ciberataque e as suas características.



Concluindo este capitulo, após ter apresentado uma serie de estudos relativamente à estrutura de uma ameaça, as suas características, e o modus operando mais conhecido, considero importante, para justificar o objetivo deste trabalho, o desenvolvimento de um quadro situacional para a cibersegurança em Portugal, apresentar a minha pesquisa realizada de modo a dar a entender quais são as características de um modelo de maturidade desejadas para um centro de cibersegurança, e como é que estes contribuem para o desenvolvimento do quadro situacional que se pretende obter.

4. Características de um modelo de maturidade de um centro de cibersegurança

As organizações deviam avaliar regularmente a maturidade das suas capacidades de cibersegurança e identificar oportunidades para melhorar a sua postura de segurança através da partilha de informação e coordenação. O propósito deste capítulo é o de descrever as características de um modelo de cibersegurança maturo e o processo pelo qual uma organização se pode tornar tanto consumidor como produtor de "Actionable threat intelligence".

"A maturidade das operações de cibersegurança de uma organização é determinada pela sua habilidade de estabelecer e gerir uma cultura operacional e uma infraestrutura necessária para gerir ativamente riscos de cibersegurança." Carson Zimmerman, (2014).

Uma organização tem de compreender as ameaças de segurança aos seus sistemas, ativos, dados, e capacidades e priorizar os seus esforços, consistentes com a sua estratégia de gestão de risco e necessidades. Uma organização deve desenvolver e implementar medidas proactivas para mitigar o impacto de incidentes potenciais á sua segurança, implantar medidas que permitam a deteção e resposta a incidentes de segurança a tempo, e serem capazes de rapidamente restabelecer as suas capacidades ou serviços que tiverem sido afetados por um incidente de segurança.

Uma organização devia mudar de abordagens de segurança reativas informais onde a organização opera em isolação para medidas formais, adaptáveis,

proactivas, com conhecimento de risco onde a organização coordena e colabora com os seus parceiros. As equipas de cibersegurança devem usar as informações remetentes de fontes internas e externas para desenvolver e implementar medidas proactivas eficazes, detetar reconhecimento de redes e ataques, identificar ameaças, vulnerabilidades, e indicadores de compromisso; e responder e recuperar de ciberataques. Organizações que possuam equipas bem treinadas estão em melhor posicionadas para influenciar oportunidades de partilha e coordenação.

Ao participarem em relações de partilha de informação, uma organização tem acesso a uma extensa coleção de cyber threat intelligence que pode ser usada para reforçar as suas defesas. No entanto, uma organização que participa nesta relação de partilha de informação não deixa de ter necessidade de implementar as suas próprias medidas de cibersegurança; tem ainda que desenvolver a sua experiencia e infraestruturas para produzir threat intelligence interno e conseguir agir sobre a informação que recebe de fontes externas. A partilha e coordenação só é eficaz se a pessoa ou organização em causa conseguir obter resultados da informação partilhada; a informação é utilizável quando uma organização possui os recursos essenciais através da qual a informação partilhada consegue influenciar a deteção, analise, resposta, e esforços de recuperação. Por exemplo, threat intelligence partilhada que contenha elementos de dados, tais como, adereços de IP, tem a habilidade de aplicar esta informação a um sensor, e pode identificar que pontos da rede sofreram impacto. Outro exemplo, uma organização pode receber threat intelligence ao reportar que uma vulnerabilidade pode ser detetada ao observar se a presença de um artefacto específico no sistema ou uma configuração num certo valor. Se a organização não tiver intenções de monitorizar artefactos no sistema ou configurações, a informação partilhada não tem valor imediato para a organização.[27] Sem as suas capacidades essenciais de

[27] The Cybersecurity Framework Tiers describe the degree to which an organization's cybersecurity risk management practices exhibit these characteristics (e.g., risk and threat aware, repeatable, and adaptive).See the Framework for Improving Critical Infrastructure Cybersecurityfor additional information,

cibersegurança bem estruturadas, a partilha e coordenação de informação não vão trazer grandes benefícios á organização, tendo em conta de que a informação recebida não é utilizável.

4.1. Consumidor, produtor, e capacidade evolutiva

Geralmente, iniciantes numa comunidade de partilha são na sua maioria, mais consumidores de threat intelligence do que produtores de informação. As comunidades de partilha beneficiam da partilha de informação dinâmica e simétrica, por isso uma organização deveria procurar evoluir de apenas consumidor para ambos consumidor e produtor de threat intelligence. Ao produzir threat intelligence, uma organização ganha mais experiencia, ajuda as outras organizações mais eficazmente a responder a ameaças no seu sector, e fomenta a confiança com os outros membros da comunidade.

Existem alguns passos a seguir no sentido de uma organização adquirir a maturidade necessária para se tornar uma organização capaz de consumir, desenvolver, e partilhar cyber threat intelligence. Os passos para esta progressão são descritos abaixo:

1. **Estabelecer os recursos essenciais de cibersegurança.** Uma organização deve implementar uma infraestrutura e os processos necessários para suportar as capacidades essenciais de cibersegurança requeridos para participar em atividades de partilha de informação e colaboração com outras entidades. Estas capacidades essenciais incluem uma infraestrutura de monotorização que seja eficaz na deteção, análise e resposta de incidentes. Um exemplo é implementar meios de monotorização da rede

periférica tal como um sistema de deteção de intrusões (IDS)[28] ou um antivírus de rede (AV)[29].

2. **Estabelecer e participar em relações de partilha e coordenação com outras entidades.** Uma organização deve identificar fontes externas de informação que sejam capazes de aumentar a base de dados interna sobre threat intelligence, que servirá para aumentar o valor da mesma e partilhar com membros da comunidade.

3. **Utilizar threat intelligence fornecida por fontes externas.** Uma organização deve ser capaz de estabelecer a infraestrutura, a logística necessária para consumir threat intelligence básica (ex., indicadores simples como endereços IP, domínios) partilhada pelos seus parceiros. Fontes externas de threat intelligence podem incluir feeds de fontes comercias, sectoriais, ou feeds de vulnerabilidades, ameaças e assinaturas de fontes abertas.

4. **Desenvolver threat intelligence básica.** Uma organização deve ser capaz de estabelecer uma infraestrutura capaz de produzir "basic threat intelligence" e divulga lo, como achar apropriado, pelos seus parceiros.

5. **Usar threat intelligence para suportar processos de tomada de decisão.** Uma organização deve integrar a threat intelligence recebida de ambas as fontes internas e externas nos seus recursos de resposta a

[28] IDS- IDS -Sistema de deteção de intrusos ou também conhecido como Sistema de deteção de intrusão (em inglês: Intrusion detection system - IDS) refere-se aos meios técnicos de descobrir em uma rede acessos não autorizados que podem indicar a ação de um *cracker* ou até mesmo de funcionários mal-intencionados. Com o acentuado crescimento das tecnologias de infraestrutura tanto nos serviços quanto nos protocolos de rede torna-se cada vez mais difícil a implantação de sistema de deteção de intrusos. Esse fato está intimamente ligado não somente a velocidade com que as tecnologias avançam, mas principalmente com a complexidade dos meios que são utilizados para aumentar a segurança nas transmissões de dados. Uma solução bastante discutida é a utilização de *host-based* IDS que analisam o tráfego de forma individual em uma rede. No *host-based* o IDS é instalado em um servidor para alertar e identificar ataques e tentativas de acessos indevidos à própria máquina.

[29] AV- Os antivírus são programas de computador concebidos para prevenir, detetar e eliminar vírus de computadores. Existe uma grande variedade de produtos com esse intuito no mercado, sendo recomendado utilizar apenas um antivírus gratuito ou apenas um pago. A diferença está nas camadas a mais de proteção que a versão paga oferece, além do suporte técnico realizado pela equipe especializada.

incidentes. Por exemplo, uma organização pode implantar IDS melhorados, expandir as atividades de monotorização e avaliação, ou bloquear endereços de IP de acordo com threat intelligence que representam. A organização deve usar a threat intelligence para ajudar a priorizar a ações de resposta, melhorar os recursos de deteção, e a desenvolver e implementar ações eficazes.

6. **Partilhar threat intelligence com outras entidades parceiras.** Uma organização deve estabelecer uma infraestrutura, processos e o treino necessário para disseminar threat intelligence, apropriadamente, para partilhar com os seus parceiros.

7. **Desenvolver e implementar recursos avançados de cibersegurança.** Em determinados casos, as fontes externas vão possuir threat intelligence que uma organização não consegue utilizar devido a falta de experiencia ou recursos da sua infraestrutura. Nesses casos, a threat intelligence só estará disponível depois de a organização expandir o âmbito da sua monotorização (ex., monitorizar novas fontes ou informação adicional ou uma maior frequência), desenvolvimento das suas competências, ou implantar ferramentas de segurança mais eficazes. Por exemplo, o host de monitorização da organização pode não estar configurado ou ser capaz de analisar certos artefactos do sistema e algumas configurações de interesse. Alem disso, assim que uma organização começa a participar mais com os seus membros da comunidade (peers), a relação de confiança entre ambas aumenta o que pode ajudar a promover a troca de conhecimento técnico. Um exemplo de recursos avançados é criar uma equipa de forense que faça um trabalho detalhado na rede e maquinas e uma análise detalhada de malware; a implementação de recursos defensivos como honeypots[30],

[30] Honeypots- (tradução livre para o português, Pote de Mel) é uma ferramenta que tem a função de propositalmente simular falhas de segurança de um sistema e colher informações sobre o invasor. É uma espécie de armadilha para invasores. O HoneyPot, não oferece nenhum tipo de proteção.

honeynets[31]; ou implementar funções avançadas de análise e visualização que ajudem a expor a TTPs do atacante.

8. **Utilizar threat intelligence "avançada" de fontes externas.** Uma organização deve estabelecer uma infraestrutura, os processos, e o treino necessário para conseguir utilizar threat intelligence avançado. (ex., TTPs, NetFlows[32]) dos seus parceiros da comunidade de partilha.

9. **Produzir threat intelligence avançado.** Uma organização deve estabelecer uma infraestrutura, os processos, e o treino necessário para conseguir produzir threat intelligence avançado (ex., TTPs, artefactos de malware). Uma organização ao desenvolver novas fontes de threat intelligence e novas técnicas analíticas vai ganhar a experiencia necessária para criar e publicar threat intelligence avançado e a capacidade de fazer uma análise de uma forma mais detalhada e sofisticada sob os incidentes.

10. **Utilizar threat intelligence avançado para suportar o processo de tomada de decisão.** Uma organização deve integrar a threat intelligence avançada que recebe de ambas as fontes internas e externas nos seus recursos de resposta a incidentes. A utilização da threat intelligence avançada vai permitir ao analista do SOC responder á ameaça logo no início do ciclo do ataque e implementar as medidas de prevenção ou correção necessárias para evitar ou bloquear o mesmo de atingir os seus objetivos.

11. **Partilhar threat intelligence avançado com parceiros externos.** Organizações que produzem threat intelligence avançado possuem informação que pode beneficiar outros e deve partilha la com os seus parceiros sempre que possível. Ao agir como produtor e publicador de

[31] Honeynets -são redes compostas de uma sub-rede de administração e de uma sub-rede de honeypots

[32] NetFlows- é um recurso que foi introduzido em roteadores Cisco cuja função é coletar o tráfego de redes IP, tanto na saída quanto na entrada de uma interface. Ao analisar os dados fornecidos pelo Netflow, um administrador de rede pode determinar tarefas como a origem e o destino do tráfego, classe de serviço, e as causas de congestionamento. Netflow é composto por três componentes: a cache de fluxo, coletor de fluxo e analisador de dados.

informação a organização vai contribuir com nova threat intelligence á comunidade ou enriquece la.

4.2. Princípios fundamentais e recursos infraestruturais

A participação numa partilha de informação e coordenação de incidentes pode requerer algumas alterações nas políticas organizacionais e procedimentos, nos recursos implementados e no treino do pessoal da organização em causa. Uma organização deve estabelecer as bases e infraestrutura necessária para manter a sua postura de segurança, e identificar funções e responsabilidades para instalar, operar, e manter esses recursos. Os princípios fundamentais e infraestruturais, no seu nível mínimo, incluem:

- **Organização estrutural para coordenação de incidentes.** Uma organização deve ter politicas que: (i) definam as estruturas de gestão, funções, responsabilidades, e responsabilidades, e a autoridade conferida ao pessoal da equipa de resposta a incidentes; (ii) descrever os procedimentos de não interferência e agravamento entre membros da equipa e equipas; (iii) identificar os mecanismos primários e de ressalva que permitam ao pessoal de resposta a incidentes se coordenarem eficazmente com ambas as partes interessadas, internas e externas.
- **Ativos, Vulnerabilidades e Administração de sistemas.** Uma organização deve possuir capacidades rudimentares de gestão de ativos, vulnerabilidades e administração de sistemas em ordem para assegurar de que a organização consegue, ativamente, monitorizar e gerir o hardware e software das suas redes e assegurar que as vulnerabilidades são remendadas a tempo.

- **Armazenamento de logs e alertas.** Uma infraestrutura que suporte a recolha dos logs e alertas gerado pelos sistemas de segurança de toda a empresa ou organização. A capacidade de recolha deve fornecer uma cobertura ampla da infraestrutura da rede da empresa/organização; permitir que novas fontes de dados de logs sejam incorporados de forma simplificada; e permitir que o analista mude o tipo de dados recolhidos, a frequência da recolha, ou de descontinuar a recolha de certos elementos não relevantes.
- **Pesquisa e recuperação de logs e alertas.** As organizações devem considerar a utilização de soluções de segurança de informação e gestão de eventos para agregar, analisar, e correlacionar dados de logs e alertas e que forneça situational awareness á equipa de resposta a incidentes e que os permita pesquisar e recuperar dados dos logs e alertas e usar essa informação para detetar atividades maliciosas, proteger o sistema e a informação, e suportar a resposta a incidentes.
- **Ferramentas de resposta.** Uma organização deve ter a infraestrutura e ferramentas necessárias para mitigar, e recuperar de um ciberataque. Isto inclui ferramentas e infraestrutura para contingência (ex., sandbox network[33]), ferramentas de análise forense, remoção de malware, e backups do sistema frequentes para suportar quaisquer esforços de recuperação.

[33] Sandbox network- O conceito do Sandbox é bem semelhante ao de criar uma máquina virtual – de fato, esse método é considerado um tipo de virtualização. Porém, esse sistema é muito mais focado em segurança; assemelhando-se, de certa forma, ao modo privativo dos navegadores. Isso fica claro pela principal característica dos aplicativos Sandbox: todos os registros e danos causados pelo que quer que seja executado dentro dele é imediatamente apagado assim que seu computador for reiniciado. Além disso, esses programas não precisam que um segundo sistema seja iniciado, permitindo que seu PC seja utilizado normalmente e sem perda de desempenho.

4.3. Recursos essenciais de cibersegurança

Organizações com a sua infraestrutura base estabelecida devem monitorizar a sua infraestrutura, e estabelecer uma base para os seus usuários, sistema e atividades na rede. Ao se estabelecer uma base, os sensores podem ser configurados para criarem alertas quando observarem comportamentos e atividades significativamente afastados da base estabelecida.

Os recursos essenciais de cibersegurança incluem:

- **Implantar, configurar, monitorizar, e atualizar os sensores.** Uma organização deve ter sensores nos hosts capazes de armazenar informação relativa ao estado dos processos, portas, ficheiros, serviços, hardware, software, e configuração dos terminais do sistema, e deveria ter sensores nas redes capazes de monitorização ativa/passiva das atividades na rede para fornecer um situational awareness otimizado. O pessoal de operações deve rever e responder aos alertas gerados por estes sensores e atualizar as assinaturas dos ficheiros e a configuração destes dispositivos para abordar falsos positivos/negativos e abordar ameaças emergentes.
- **Gerir dados dos logs.** Uma organização deve gerar, armazenar, agregar, e gerir logs relevantes, alertas, e informação sobre eventos de toda a organização. Uma organização pode usar um servidor dedicado a logs, software gestor de logs, ou um produto de segurança de informação e gestão de eventos para permitir a recolha eficaz, a agregação, analise, e armazenamento dos dados dos logs.

- **Documentação, priorizar, e gerir incidentes.** Uma organização deve ter procedimentos de resposta a incidentes que documentem o processo de tratamento dos incidentes. Estes procedimentos devem cobrir todas as fases do ciclo de vida da resposta ao incidente.
- **Realizar análise forense básica de trafego de rede.** Uma organização deve possuir ferramentas (ex., sniffer[34]), dados de logs e a experiencia necessária para correlacionar e analisar eventos de rede; identificar técnicas comuns de atacantes como Scanning de portas, sondas, e falsificação de endereços IP[35]; e deve possuir conhecimento básico de como os atacantes usam portas específicas, protocolos, e serviços para realizar ataques.
- **Coordenação com responsáveis dos sistemas.** Uma organização deve ter os processos e mecanismos de comunicação necessários que permita á equipa de resposta a incidentes comunicar eficazmente com os "donos" dos sistemas durantes um incidente ativo. Os "donos" ou responsáveis por esta rede/sistema podem ter de ser consultados quando as decisões de resposta tomadas possam causar a interrupção dos seus serviços ou tiver algum outro impacto a nível operacional.

[34] Sniffer-, em rede de computadores, é o procedimento realizado por uma ferramenta conhecida como *Sniffer* (também conhecido como *Packet Sniffer*, *Analisador de Rede*, *Analisador de Protocolo*, *Ethernet Sniffer* em redes do padrão Ethernet ou ainda *Wireless Sniffer* em redes *wireless*). Esta ferramenta, constituída de um *software* ou *hardware*, é capaz de intercetar e registrar o tráfego de dados em uma rede de computadores. Conforme o fluxo de dados trafega na rede, o *sniffer* captura cada pacote e eventualmente decodifica e analisa o seu conteúdo de acordo com o protocolo definido em um RFC ou uma outra especificação. O *sniffing* pode ser utilizado com propósitos maliciosos por invasores que tentam capturar o tráfego da rede com diversos objetivos, dentre os quais podem ser citados, obter cópias de arquivos importantes durante sua transmissão, e obter senhas que permitam estender o seu raio de penetração em um ambiente invadido ou ver as conversações em tempo real.

[35] IP Spoofing- No contexto de redes de computadores, IP spoofing é um ataque que consiste em mascarar (spoof) pacotes IP utilizando endereços de remetentes falsificados. Devido às características do protocolo IP, o reencaminhamento de pacotes é feito com base numa premissa muito simples: o pacote deverá ir para o destinatário (endereço-destino) e não há verificação do remetente — não há validação do endereço IP nem relação deste com o router anterior (que encaminhou o pacote). Assim, torna-se trivial falsificar o endereço de origem através de uma manipulação simples do cabeçalho IP. Assim, vários computadores podem enviar pacotes fazendo-se passar por um determinado endereço de origem, o que representa uma séria ameaça para os sistemas baseados em autenticação pelo endereço IP.

Resumindo a informação referida neste capítulo temos alguns pontos-chave que merecem ser destacados.

Uma organização deve ter, ou desenvolver, os princípios fundamentais e infraestrutura estabelecida para suportar a partilha de informação e coordenação de atividades; procurar fontes externas de informação e entrar em varias relações de partilha de informação e coordenação á medida de que o seu modelo de maturidade matura; consumir informação de fontes externas e aplicar a informação recolhida para melhorar os seus recursos internos de resposta a incidentes; expandir a sua recolha de informação interna, realizar análises mais sofisticadas, e começar a desenvolver e publicar os seus próprios indicadores, e deve realizar autoavaliações de rotina para identificar oportunidades para melhorar as suas medidas de cibersegurança.

De modo a atingir estes objetivos dentro de uma organização, é fundamental, criar e desenvolver relações de partilha de informação com outras organizações parceiras. No próximo capitulo, vou apresentar uma serie de propostas de modelos de partilha de informação que considero importantes para o desenvolvimento da maturidade de uma organização e essenciais para o desenvolvimento de um quadro situacional para a cibersegurança em Portugal.

5. Arquiteturas de partilha de informação para comunidades de cibersegurança

No capítulo anterior referi as características fundamentais de um centro de cibersegurança para atingirem o seu estado de maturidade. Neste capítulo vou abordar o tema de partilha de informação, como processo vital ao bom funcionamento de um centro de cibersegurança, com a comunidade de TIC e outras forças relevantes em matéria de cibersegurança.

Grande parte das comunidades de partilha trocam informação entre si, utilizando algumas das variáveis arquiteturas básicas de partilha de informação; (i) centralizada; e (ii) peer-to-peer. Os requisitos de partilha de informação para uma comunidade ajudam a determinar qual a arquitetura mais adequada para a mesma. Algumas comunidades podem beneficiar de uma arquitetura mais centralizada; outras, podem preferir trocar informações diretamente entre partes (peer-to-peer); ainda assim outros podem utilizar um modelo no qual estejam incorporados características de ambas as arquiteturas. Quando se está a determinar que arquitetura é a mais adequada para uma comunidade, são precisos ter em consideração alguns fatores chave:

- As características, fiabilidade, capacidade, e a composição dos participantes
- O nível de compromisso do governo, das organizações membros, e patrocínios para suportar as comunidades
- O tipo e sensibilidade da informação que vai ser partilhada
- A frequência, volume, e velocidade da distribuição da informação

5.1. Arquitetura Centralizada

A arquitetura centralizada é geralmente descrita como “hub-and-spoke”, onde a “hub” central, serve de repositório ou filtragem da informação que recebe dos “spokes” (i.e., membros participantes) ou outras fontes. Informação fornecida ao “hub” pelos membros participantes pode ser diretamente enviada para os outros membros da comunidade (i.e. não processada) ou o “hub” pode melhorar a qualidade de informação de alguma forma e depois distribui-la aos membros da comunidade designados. As melhorias realizadas pelo “hub” podem incluir agregação e correlação de informação de múltiplas fontes, sanitização, enriquecimento da informação ao fornecer contexto adicional, ou tendências e analises que identifiquem tendências comuns, ameaças, e atividades maliciosas dentro da comunidade geral.

Comunidades de partilha baseadas nesta arquitetura, normalmente estabelecem acordos formais de partilha de dados que estipulam que informação pode ser partilhada, com quem pode ser partilhada, a quem e permitida a atribuição e o nível de detalhe permitido. A informação recebida pelo repositório central pode ser bastante detalhada, volumosa, e conter elementos de informação que permitam a sua atribuição. Os processos de sumarização do repositório, sanitização e distribuição devem tratar a informação de acordo com os acordos de partilha de informação. Repositórios centrais que recebem frequentemente, grande volume de pedidos podem escolher automatizar alguns processos de sumarização e sanitização.

Os benefícios conferidos de uma arquitetura “hub-and-spoke” são na sua maioria determinados pelos serviços realizados pelo “hub”. Os serviços fornecidos pelo “hub” central podem variar de comunidade para comunidade; alguns “hubs” podem simplesmente servir de corretores da troca de informações, outros podem realizar processos adicionais para enriquecer a informação. Numa comunidade “hub-and-spoke” os serviços do “hub” central podem incluir consumo,

agregação, correlação, analise, validação, sanitização, distribuição, e arquivamento de informação de uma variedade de fontes.

"Hubs" que usam formatos de "standard data" abertos e protocolos de transporte, aliviam a necessidade de os participantes de adotarem múltiplos formatos e protocolos de troca de informação com outros membros da comunidade. Assim, os participantes tem menos ligações para gerir – uma vez que exista uma ligação ao "hub", os membros da comunidade ficam interligados através da infraestrutura do "hub".

O custo da infraestrutura do "hub" é geralmente coberto por taxas pagas pelos membros ou pelos serviços prestados. Se estas taxas forem muito altas, podem representar uma barreira a entrada e dificultarem a participação de certas organizações nesta comunidade. Uma potencial desvantagem nesta arquitetura é o facto do sistema de partilha de informação estar totalmente dependente da infraestrutura do "hub", tornando a vulnerável a falhas do sistema, atrasos (ex., devido a congestionamento na rede, eventos por processar, ou a contenção de outros recursos), ou o "hub" ser comprometido. Embora a sensibilidade da informação variar com o tempo, quando o "hub" não esta a funcionar, ou o seu funcionamento esta afetado de alguma forma, todos os membros da comunidade são afetados. Uma consideração final a ter é a de que, o "hub" como um repositório de threat intelligence, se torna assim um alvo apetecível para atacantes.

5.2. Arquitetura Peer-to-Peer

Em vez de encaminharem os dados através de um "hub" central, membros peer-to-peer partilham diretamente entre si. Uma vez que não existe um "hub", cada organização é responsável pelo consumo, agregação, correlação, analise, validação, sanitização, proteção, e partilha de informação com os seus peers. A informação que é partilhada entre peers esta limitada a informação recolhida, analisada e disseminada pelos seus membros. A dinâmica da partilha de

informação (ex., segurança, velocidade e frequência) vai variar de acordo com os requisitos e capacidade dos peer.

Numa relação peer-to-peer, a confiança é diretamente estabelecida entre os peers em vez de ser organizada através de um repositório central. Baseado no nível de confiança estabelecido e no tipo de informação em causa, uma organização pode escolher partilhar com um membro específico da comunidade, um grupo designado de recipientes, ou com todos os peers. A confiança peer-to-peer baseia se no princípio de que os peers apoiam uma missão comum, respeitam as regras estabelecidas, e demonstram vontade em participar numa partilha reciproca.

A arquitetura peer-to-peer traz vários benefícios: (i) os participantes peer-to-peer partilham entre si (ex., sem intermediário como o "hub"); isto oferece maior agilidade e permite que a informação seja rapidamente distribuída pois o participante recebe a informação diretamente da fonte. (ii) Arquiteturas peer-to-peer demonstram geralmente uma maior resiliência tendo em conta de que a informação esta disponível através de múltiplos canais de comunicação e não existe um hub central que represente um potencial ponto único de falha ou um potencial alvo de ataques.

A arquitetura peer-to-peer tem algumas inconveniências incluindo: (i) implementações peer-to-peer que não utilizem os métodos padrão de partilha de informação são difíceis de medir considerando que os "peers" tem de suportar múltiplos formatos e protocolos (ii) Á medida de que o número de membros peer-to-peer aumenta, os custos operacionais de gestão das numerosas conexões, data (ex., consumo, agregação, correlação, analise, validação, filtragem, proteção e partilha), podem crescer exponencialmente.

A partilha de informação entre uma organização e o seu provedor de internet (ISP)[36], Administrador, sócios, parceiros do sector industrial, forças policiais e agências governamentais, e outras equipas de resposta a incidentes, geralmente

[36] ISP- Fornecedor de acesso à Internet é a tradução para IAP (*Internet access provider*). IAP é uma outra maneira pela qual nos referimos ao ISP (*Internet Service Provider*) cuja tradução é "Provedor de serviços de Internet". Que não configura ambiguidade pois os serviços são providos através dele e não por ele.

consistem em interações peer-to-peer. Tal partilha, apesar de não ser orquestrada através de uma comunidade de partilha, é igualmente um componente importante para uma capacidade de resposta eficaz a incidentes.

5.3. Implementações Hibridas

As duas arquiteturas previamente descritas, são de vez em quando comuns em implementações hibridas que combinam características de hub-and-spoke e peer-to-peer. Existem ambas as implementações centralizadas e descentralizadas peer-to-peer. Numa implementação peer-to-peer centralizada, um servidor central pode ser utilizado para descobrir recursos, para gerir pedidos, ou como uma terceiro membro de confiança para autentificações. Numa implementação puramente descentralizada, os participantes gerem todos os aspetos das suas interações com as pessoas da comunidade.

Uma organização, por exemplo, pode trocar indicadores de intrusões de baixo nível usando a arquitetura peer-to-peer mas enviar relatórios de incidentes high-level para um hub central. Outro cenário envolve enviar a mesma informação diretamente para certos membros do grupo, e para o hub central. Esta abordagem permite ambas, uma resposta tática eficaz (ex., ações rápidas sob informações urgentes, através de uma partilha direta e conjunta) e dá uso á capacidade do hub de recolher, combinar, e analisar dados recebidos de múltiplos membros para desenvolver estratégias a longo prazo e medidas de ação. Embora a utilização de uma abordagem hibrida possa ser vantajosa em alguns casos, também se pode tornar muito dispendiosa e difícil de implementar.

5.4. Comunidades Formais vs Informais

Comunidades de partilha de informação demonstram vários graus de formalidade. Vou descrever algumas das características das comunidades formais e informais.

Comunidades de partilha informais são geralmente grupos auto-organizados que operam através de cooperação voluntaria. Os membros são variáveis (ex., não existem membros fixos), algumas vezes anónimos, e os membros mantem anonimato total com o mínimo de coordenação central. Estas comunidades utilizam acordos de partilha de informação informais (ex., regras de conduta em vez de acordos juridicamente vinculados) que estabelecem os perímetros básicos para a partilha de informação com a comunidade.

Os participantes numa comunidade informal publicam informação no repositório voluntariamente, ad-hoc e são reesposáveis por assegurar que o conteúdo submetido no repositório é adequado para partilha. Os operadores do repositório mantem o repositório mas geralmente não fazem quaisquer asserções relativas á qualidade e relevância da informação contida no repositório; a fiabilidade na informação é baseada na reputação da pessoa que a submete. Organizações que desejam consumir informação subscrevem se a fontes de informação específicas administradas pelo repositório (ex., email, RSS feed).

Comunidades de partilha formais são geralmente organizadas a volta de uma característica comum (ex., sector industrial) e tem requisitos oficiais para os seus membros que podem ser:

- Elegibilidade para instituições (ex., sector industrial especifico)
- Elegibilidade para pessoas (ex., tem de ter responsabilidades de segurança na empresa)
- Requisitos de nomeação ou patrocínio (isto é, confiança intermediada)
- Período de membro estagiário

- Capacidades mínimas a nível de cibersegurança para a organização

A associação neste tipo de comunidades é geralmente fixada com a volatilidade mínima nas listas de assinaturas. A partilha de informação dentro da comunidade é gerida através de SLAs[37], NDAs[38], e outros acordos. Algumas comunidades recolhem uma taxa anual dos associados para cobrir os custos administrativos e serviços da comunidade.

Os pontos-chave apresentados neste capítulo são sumarizados em baixo:

Tirar o melhor proveito do conhecimento, experiencia, e das capacidades dos outros membros da comunidade para a partilha de threat intelligence, estratégias de mitigação, e ferramentas, para melhorar a cibersegurança das organizações participantes e reduzir o custo sofrido pelos ciberataques.

Estabelecer e manter relações de partilha de informação para melhorar o situational awareness das organizações e para fomentar uma abordagem proactiva na resposta a incidentes.

Utilizar o ciclo de vida de um ciberataque como um quadro para observar e compreender as ações dos atacantes e para definir uma estratégia ativa de defesa que dê uso á informação em ambas as fontes interna e externa disponíveis ao longo do ciclo de vida de um ataque.

Partilhar informação relativamente a tentativas de intrusão (independentemente de terem sido ou não intrusões com sucesso) em vez de informação sobre uma intrusão específica. Informações sobre tentativas de intrusão são menos sensíveis

[37] SLAs- Um **Acordo de Nível de Serviço** (**ANS** ou *SLA*, do inglês *Service Level Agreement*) é um acordo firmado geralmente, haja vista que outras áreas da empresa também podem se beneficiar desse recurso, entre a área de TI e seu cliente *interno*, que descreve o serviço de TI, suas metas de nível de serviço, além dos papéis e responsabilidades das partes envolvidas no acordo.

[38] NDAs- Um **acordo de não divulgação** (**Non-Disclosure Agreement** ou **NDA** em inglês, língua onde também é conhecido por **Confidential Disclosure Agreement** ou **CDA**), **termo de confidencialidade** ou **acordo secreto**, é um contrato legal entre ao menos duas partes que destacam materiais ou conhecimentos confidenciais que as partes desejam compartilhar para determinado propósito, mas cujo uso generalizado desejam restringir.

e requerem menos filtragem e analise; assim sendo, podem ser partilhadas mais rapidamente.

- Diferentes arquiteturas de partilha existem com o propósito de partilhar informação (ex., centralizadas ou peer-to-peer), e um membro desta comunidade conhece ambas as vantagens e desvantagens destas arquiteturas.
- Procurar fontes de threat intelligence que tenham informação que seja oportuna, relevante, precisa, especifica, e utilizável.

5.5. Arquitetura do Modelo de Coordenação e Partilha de Informação do Centro Nacional de Cibersegurança

O Centro Nacional de Cibersegurança como entidade coordenadora[39],como referido na estratégia nacional de cibersegurança[40], compete-lhe promover e assegurar a articulação e a cooperação entre os vários intervenientes e responsáveis nacionais na área da cibersegurança, assegurar a produção de referenciais normativos em matéria de cibersegurança e coordenar a partilha de informações entre entidades.

A arquitetura de partilha de informação em causa pode ser considerada, uma arquitetura hibrida. Tendo em conta de que o centro funciona, em certos casos, como "hub-and-spoke" e distribui a informação como achar relevante para as

[39] Decreto-Lei Nº 69/2014- Artigo 2.º-A, "Competências do Centro Nacional de Cibergurança
i) Coordenar a cooperação internacional em matérias da cibersegurança, em articulação com o Ministério dos Negócios Estrangeiros;"

[40] Estratégia Nacional de Cibersegurança em anexo

outras entidades ou “peers”, geralmente quando se trata de informações provenientes de fontes externas. Mas também, funciona num modelo “peer-to-peer” com as entidades competentes em matéria de cibersegurança, quando se trata de informações provenientes de fontes internas.

Esta partilha de informação é importante para aumentar o nível de awareness das várias entidades, partilhando entre si quaisquer conhecimentos sobre ameaças e vulnerabilidades aos seus sistemas, para que estas possam ser evitadas ou remediadas.

6. Autoridades competentes em matéria de Cibersegurança Nacional

Em matéria de Cibersegurança Nacional existem varias entidades que contribuem para o bom funcionamento do ciberespaço, da segurança e do cumprimento das leis, os quais vou referenciar nesta capitulo seguido de uma descrição breve das suas respetivas competências.

6.1. Centro Nacional de Cibersegurança

O Centro Nacional de Cibersegurança (CNCS) é um órgão integrado no Gabinete Nacional de Segurança sob a tutela da Presidência do Conselho de Ministros, o qual tem a responsabilidade de desenvolver as capacidades nacionais de prevenção, monitorização, deteção, reação, analise e correção destinadas a fazer face a incidentes de cibersegurança e ciberataques.
Atua em articulação e estreita cooperação com as estruturas nacionais responsáveis pela ciberespionagem, ciberdefesa, cibercrime e ciberterrorismo, devendo comunicar à Polícia Judiciária, no mais curto prazo, os factos de que tenha conhecimento relativos à preparação e execução de crimes. No quadro de competências do CNCS destacam se o desenvolvimento de capacidades nacionais de prevenção, monitorização, deteção, reação, análise e correção destinadas a fazer face a incidentes de cibersegurança e ciberataques; a promoção de formação e a qualificação de recursos humanos na área da cibersegurança, com vista à formação de uma comunidade de conhecimento e de uma cultura nacional de cibersegurança; exercer os poderes de autoridade nacional competente em matéria de cibersegurança, relativamente ao Estado e aos operadores de infraestruturas críticas nacionais; assegurar o planeamento da utilização do ciberespaço em situação de crise e de guerra no âmbito do

planeamento civil de emergência[41] e coordenar a cooperação internacional em matérias da cibersegurança, em articulação com o Ministério dos Negócios Estrangeiros.

6.2. Autoridade Nacional de Segurança / Gabinete Nacional de Segurança

O Gabinete Nacional de Segurança (GNS) é dirigido pela Autoridade Nacional de Segurança (ANS) a quem compete superintender tecnicamente os procedimentos da administração pública e garantir o cumprimento das medidas para garantia da segurança das matérias classificadas nacionais ou da responsabilidade nacional, designadamente as das organizações internacionais de que Portugal é parte, bem como exercer a autoridade de credenciação de pessoas e empresas para acesso e manuseamento dessas mesmas matérias. A ANS é igualmente a entidade credenciadora competente para a credenciação e a fiscalização das entidades certificadoras compreendidas no SCEE[42]

No quadro das competências do GNS[43], destacam-se a acreditação e a certificação de segurança de produtos e sistemas de comunicações, de informática e de tecnologias de informação que sirvam de suporte ao tratamento, arquivo e transmissão de matérias classificadas; a promoção do estudo, investigação e difusão das normas e procedimentos de segurança aplicáveis à

[41] Decreto-Lei n.º 73/2013, de 31 de maio

[42] Cf. Decreto-Lei n.º 116-A/2006 de 16 de Junho. De notar que os termos usados no n.º 1 do art.º 8.º do mesmo Decreto-Lei referem a Autoridade Nacional de Segurança como autoridade credenciadora nacional para as entidades certificadoras compreendidas no SCEE, ou seja, a entidade de certificação eletrónica do Estado e as entidades certificadoras do Estado nelas admitidas. Esta formulação leva-nos a admitir que o ITIJ mantém as funções de autoridade credenciadora para as restantes entidades certificadoras que não as compreendidas no SCEE, nomeadamente as entidades privadas. No entanto quer o preâmbulo do diploma, quando refere que compete [...] à Autoridade Nacional de Segurança as funções de autoridade credenciadora, que até agora se encontravam atribuídas ao Instituto das Tecnologias da Informação da Justiça, quer a norma revogatória, a que se refere o art.º 8.º do mesmo diploma, e que retira da Lei Orgânica do Ministério da Justiça a competência do ITIJ nesta matéria, são claros

[43] Cf. Decreto-Lei n.º 170/2007 de 3 de Maio

proteção e salvaguarda das matérias classificadas, propondo a doutrina a adotar por Portugal na matéria e a formação de pessoal especializado nesta área da segurança.

O GNS funciona no âmbito da Presidência do Conselho de Ministros, junto do Gabinete Coordenador de Segurança. A ANS funciona na dependência direta do Primeiro-Ministro.

6.3. Sistema de Segurança Interna

O Sistema de Segurança Interna (SSI), foi criado pela revisão de 2008 da Lei de Segurança Interna[44]. São órgãos do SSI o Conselho Superior de Segurança Interna, o Gabinete Coordenador de Segurança e o Secretário-Geral do SSI.

Cabe ao Gabinete Coordenador de Segurança estudar e propor ao Secretário-geral políticas públicas de segurança interna e estratégias e planos de ação nacionais na área da prevenção da criminalidade. Este Gabinete é ainda responsável pela elaboração do Relatório Anual de Segurança Interna.

Ao Secretário-Geral cabe, de particular importância para a cibersegurança, a responsabilidade da articulação das forças e serviços de segurança e pela gestão de incidentes tático-policiais graves, onde se incluem os ataques contra IC ou destinadas ao abastecimento e satisfação de necessidades vitais da população[45]. Refira-se ainda que no âmbito das suas competências de coordenação, cabe ao Secretário-Geral estabelecer os mecanismos de articulação entre as várias forças

[44] Cf. Lei n.º 53/2008, de 29 de Agosto

[45] Cf. Alínea b) do n.º 2 e al. a) do n.º 3 do art.º 18.º e da Lei 53/2008, de 29 de Agosto. Esta norma atribui ao Secretário-Geral do SSI a competência de gestão de incidentes como aqueles que se verificaram na Estónia em 2006 ou na Geórgia em 2008.

e serviços de segurança, com os organismos congéneres e com outras entidades, públicas e privadas, relevantes na área da segurança. O Secretário-Geral do SSI funciona na direta dependência do Primeiro-ministro ou, por sua delegação, do Ministro da Administração Interna.

6.4. Sistema de Informações da República Portuguesa

O Sistema de Informações da República Portuguesa (SIRP) e os seus serviços de informações o Serviço de informações e Segurança (SIS) e o Serviço de Informações Estratégicas de Defesa, desempenham um papel fundamental na prevenção da criminalidade grave e das ameaças suscetíveis de fazer perigar a segurança nacional, nas suas vertentes de segurança interna e defesa nacional.

De realçar a preocupação do SIS, expressa em relatórios[46] e no seu site web relativamente às ciberameaças.[47]

[46] Ver RASI de 2010.

[47] O SIS refere como principais preocupações neste âmbito, o "recurso à Internet para a prática de atos ilícitos, designadamente ao nível da fraude e do furto de identidade, bem como o furto, movimentação e branqueamento de capitais, à escala global; Interação entre sistemas e conjuntos de sistemas Interligados em rede expondo vulnerabilidades que propiciam o surgimento de novas ameaças especialmente complexas, passíveis de exploração ilícita por grupos de criminalidade organizada no espaço virtual; Novos usos da Internet por elementos de organizações terroristas, nomeadamente nas áreas da radicalização política e ideológica, recrutamento, financiamento, planeamento e coordenação de atentados, bem como o impacto dos novos meios na evolução das dinâmicas e estruturas das organizações terroristas; Utilização do meio cibernético, por grupos terroristas, de forma ofensiva e contra infraestruturas críticas, a segurança dos cidadãos e a manutenção do Estado de Direito, tendo em vista inibir, forçar ou condicionar a ação do Estado ou de comunidades; Atos de espionagem praticados com recurso a meios eletrónicos.

O Secretário-GeraldoSIRPfuncionanadirectadependênciadoPrimeiro-Ministro ou, por delegação, num membro do governo da Presidência do Conselho de Ministros.

6.5. Policia Judiciária

A Polícia Judiciária (PJ) é o principal órgão de polícia criminal em matéria de cibercrime. A PJ tem por missão coadjuvar as autoridades judiciárias na investigação, desenvolver e promover as ações de prevenção, deteção e investigação da sua competência ou que lhe sejam cometidas pelas autoridades judiciárias competentes.[48]

De entre as suas atribuições destacam-se a realização das ações que antecedem o julgamento e que requerem conhecimentos ou meios técnicos especiais e a promoção e a realização de ações destinadas a fomentar a prevenção geral e a reduzir o número de vítimas da prática de crimes.

A PJ, nomeadamente a sua secção de investigação da criminalidade informática e tecnológica da Diretoria de Lisboa e Vale do Tejo, é ainda o órgão competente paraefeitosdecooperaçãointernacionaleopontodecontactopermanenteprevistos na Lei do Cibercrime e assegurar o funcionamento dos gabinetes da Interpol e

[48] Cf. Lei n.º 37/2008 com as alterações introduzidas pela Lei 26/2010, de 30 de Agosto.

Europol para os efeitos da sua própria missão e para partilha de informação.[49] A PJ depende hierarquicamente do Ministério da Justiça.

Neste capitulo foram apresentadas as varias entidades com competências a nível nacional em matéria de cibersegurança e as suas respetivas estruturas organizacionais. Para se compreender por inteiro este ultimo capitulo, considerei importante referir as características de um Security Operations Center (SOC), no capitulo seguinte. Considerando o objetivo principal deste trabalho, é importante salientar que para o desenvolvimento de um quadro situacional, é necessário compreender em profundidade todos os aspetos estruturais constituintes de um centro de cibersegurança. Deste modo, no capitulo seguinte, estão descritos os componentes estruturais de um SOC comum, assim como, a estrutura do Centro Nacional de Cibersegurança, de acordo com as características descritas no plano de estratégia de cibersegurança nacional na Resolução do Conselho de Ministros n.º 36/2015, de 12 de junho.

[49] Cf. Art.º 21.º e art.º 29.º da Lei 109/2009, de 15 de Setembro e n.º 2 do art.º 5.º da Lei n.º 37/2008 com as alterações introduzidas pela Lei 26/2010, de 30 de Agosto.

7. Estrutura de um Security Operations Center (SOC)

Os centros operacionais de cibersegurança (CSOC)[50] de hoje em dia devem ter tudo o que precisam para montar uma defesa competente no mundo da constante mudança da tecnologia. Isto inclui uma vasta matriz de tecnologias sofisticadas de deteção e prevenção, um mar virtual de relatórios de cyber intelligence, e uma equipa de IT experiente e trabalhadora. As cartas não jogam a favor dos responsáveis pela segurança pois enquanto os atacantes tem de descobrir uma maneira de entrar no sistema, a equipa de IT tem de segurar todas as entradas, limitar e avaliar os danos, e encontrar e remover a presença de qualquer atacante no sistema. Especialistas em cibersegurança reconhecem que atacantes sofisticados conseguem estabelecer ligações duradouras nos sistemas das organizações e/ou empresas. Como se esta situação não fosse má o suficiente, na maioria dos casos, nos somos o nosso pior inimigo. Muitos CSOC's gastam energia a combater políticas e problemas de pessoal do que a identificar e responder a ciberataques. Demasiadas vezes, CSOC's são instalados e operam mais num foco tecnológico, sem abordarem adequadamente as pessoas e os problemas processuais.

Uma equipa de um SOC pode variar de uma pequena, de cinco pessoas operacionais a uma larga, ao nível de centros de coordenação nacional. Uma missão media típica de um SOC tipicamente inclui os seguintes elementos:

[50] CSOC - Um **SOC** - **Security Operations Center** em português Centro de Operações de Segurança, é um termo genérico que descreve parte ou a totalidade de uma plataforma cujo objetivo é prestar serviços de deteção e reação a incidentes de segurança. Podemos distinguir cinco operações a serem executadas por um SOC[1] :

O principal problema encontrado na construção de um SOC é a integração de todos estes módulos e a correlação de dados que geram, comumente construídos como partes autônomas, conciliando a integridade, a disponibilidade e a confidencialidade dos dados e de seus canais de transmissão.

1. A prevenção de incidentes de cibersegurança através de:
    a. Analise contínua de ameaças
    b. Scanning de vulnerabilidades a redes e admin's
    c. Implementação e coordenação de contramedidas
    d. Políticas de segurança e consultoria de arquitetura
2. Monotorização, deteção e análise de potenciais intrusões em tempo real e através de dados de padrões de segurança relevantes registados em fontes de dados
3. Resposta a incidentes, através da coordenação de recursos e o uso direto de contramedidas precisas e relevantes
4. Fornecimento de situational awareness e relatórios sobre o estado actual de cibersegurança, incidentes, e padrões comportamentais dos atacantes relativos a organizações de interesse.
5. Desenvolver e utilizar tecnologias como IDSes[51] e armazenamento de dados / análise de sistemas

Destas responsabilidades, a mais demorada, é talvez a de armazenamento e análise da abundante quantidade de dados relevantes de segurança. Dentro dos vários feeds relevantes para o SOC, os mais prováveis de os recolherem são IDSes. IDSes são sistemas colocados ou no host ou na rede para detetarem potenciais atividades maliciosas ou atividades suspeitas que chamem a atenção

[51] IDS -Sistema de deteção de intrusos ou também conhecido como Sistema de deteção de intrusão (em inglês: Intrusion detection system - IDS) refere-se aos meios técnicos de descobrir em uma rede acessos não autorizados que podem indicar a ação de um *cracker* ou até mesmo de funcionários mal-intencionados. Com o acentuado crescimento das tecnologias de infraestrutura tanto nos serviços quanto nos protocolos de rede torna-se cada vez mais difícil a implantação de sistema de deteção de intrusos. Esse fato está intimamente ligado não somente a velocidade com que as tecnologias avançam, mas principalmente com a complexidade dos meios que são utilizados para aumentar a segurança nas transmissões de dados. Uma solução bastante discutida é a utilização de *host-based* IDS que analisam o tráfego de forma individual em uma rede. No *host-based* o IDS é instalado em um servidor para alertar e identificar ataques e tentativas de acessos indevidos à própria máquina.

do analista do SOC. Combinando logs de auditorias de segurança com outros data feeds, um SOC típico, vai coletar, analisar e armazenar dezenas ou centenas de milhões de ficheiros de eventos de segurança por dia.

Tendo em conta a definição de "evento" como "uma alteração discreta de estado num sistema, dispositivo, serviço ou estado lógico, resultante de uma ação contra um determinado alvo"

Entende-se como ação algo efetuado por um utilizador ou por um processo, com o objetivo de atingir um determinado resultado e tendo como alvo a entidade física (sistema, rede, etc…) ou lógica (informação, conta de utilizador, etc…) objeto dessa ação.

Um Evento deve ser uma situação detetada ou comunicada por um determinado sistema ou entidade e sustentado por algum tipo de prova (por exemplo logs).

Alguns exemplos de Eventos são, um scan de rede, um sistema a alojar malware, um flood distribuído de pacotes, um acesso indevido a um sistema, etc…

A cada Evento estão associados ainda uma origem e um destino, bem como um report desse Evento, no caso de este não ter sido detetado por ferramentas da instituição. Adicionalmente está ainda geralmente associado a cada Evento o instante temporal da sua ocorrência. (Cert.Pt)

7.1. CNCS - Estrutura de um SOC nacional

Obedecendo ao modelo de estrutura matricial, a Direção do CNCS conta com o apoio do Gabinete de Estratégia e Planeamento (GEP) e de três departamentos: Departamento de Operações e Controlo (DOC), Departamento de Investigação e Desenvolvimento (DID) e Departamento de Qualidade, Sensibilização e Prevenção (DQSP).

A estrutura do modelo de SOC atual do Centro Nacional de Cibersegurança dispõem dos recursos necessários para resposta a incidentes, uma equipa de analistas responsável por manter o ciberespaço nacional em segurança de quaisquer ameaças internas e externas.

Com o objetivo de desenvolver capacidades de prevenção e deteção de ameaças, esta equipa trabalha em conjunto para o desenvolvimento num projeto nacional que inclui a utilização de um sensor[52] nacional capaz de detetar quaisquer ameaças num espaço de tempo suficiente para que a equipa de resposta a incidentes a possa prevenir ou mitigar a tempo, e aumentar assim a capacidade de avaliação situacional do Centro Nacional de Cibersegurança interna e externa.

Em desenvolvimento está também um projeto que visa criar uma base de dados, para a partilha de informação necessária, *Passive DNS*[53], que armazene traduções

[52] Sensor – IDS - Sistema de deteção de intrusos ou também conhecido como Sistema de deteção de intrusão (*em inglês: Intrusion detection system - IDS*) refere-se aos meios técnicos de descobrir em uma rede acessos não autorizados que podem indicar a ação de um *cracker* ou até mesmo de funcionários mal-intencionados.

Com o acentuado crescimento das tecnologias de infraestrutura tanto nos serviços quanto nos protocolos de rede torna-se cada vez mais difícil a implantação de sistema de deteção de intrusos. Esse fato está intimamente ligado não somente a velocidade com que as tecnologias avançam, mas principalmente com a complexidade dos meios que são utilizados para aumentar a segurança nas transmissões de dados.

Uma solução bastante discutida é a utilização de *host-based* IDS que analisam o tráfego de forma individual em uma rede. No *host-based* o IDS é instalado em um servidor para alertar e identificar ataques e tentativas de acessos indevidos à própria máquina.

[53] Passive DNS - O *Domain Name System (DNS)* é um sistema de gerenciamento de nomes hierárquico e distribuído para computadores, serviços ou qualquer recurso conectado à Internet ou em uma rede privada. Ele baseia-se em nomes hierárquicos e permite a inscrição de vários dados digitados além do nome do host e seu IP. Em virtude do banco de dados de DNS ser distribuído, seu tamanho é ilimitado e o desempenho não degrada tanto quando se adiciona mais servidores nele

de DNS realizadas, a serem utilizadas no contexto de deteção, analise e reação a ciberincidentes.

De acordo com a estratégia nacional de cibersegurança vou destacar alguns pontos que considero importantes para este capítulo e para consulta, a estratégia segue na íntegra em anexo.

De acordo com os objetivos do CNCS – Centro Nacional de Cibersegurança é importante destacar, a nível de cooperação operacional, o papel de coordenação do centro como um fator operacional essencial para o sucesso da execução das medidas previstas na estratégia nacional.

O CNCS, enquanto coordenador operacional, deve desenvolver e aplicar medidas que visem a capacitação humana e tecnológica das infraestruturas publicas e das infraestruturas criticas, com vista à prevenção e à reação de e a incidentes de cibersegurança. Com vista na eficácia operacional, e a uma melhora avaliação situacional, estão em desenvolvimento os mecanismos necessários a partilha de informação de incidentes e ameaças de cibersegurança com entidades públicas e com os vários operadores das infraestruturas criticas. Ainda dentro da arquitetura de partilha está a articulação do CNCS com as autoridades competentes e a comunidade nacional de segurança do ciberespaço, como referido anteriormente, um dos projetos em desenvolvimento é o da criação de uma base de dados que reúna informação sobre ameaças e vulnerabilidades conhecidas, para servir as entidades publicas e os operadores de infraestruturas criticas.

A promoção de avaliações a maturidade e a capacidade das entidades públicas e privadas que administrem infraestruturas críticas ou serviços vitais de informação, no que respeita à segurança no ciberespaço, assim como a melhoria contínua dos sistemas de segurança dos sistemas de informação das entidades públicas, e dos operadores de infraestruturas criticas para assegurar uma maior resiliência nacional frente as ameaças existentes.

8. Liberdades e Direitos no Ciberespaço

O surgimento da internet marca o nosso tempo. O ciberespaço tem-se tornado cada vez mais o domínio através do qual as liberdades fundamentais dos cidadãos, expressão e associação são realizados, a transparência das políticas públicas é um objetivo e a eficiência da administração pública é estimulada, crescimento e inovação são alcançados. Nesta arena global virtual, milhares de milhões de conexões são realizadas todos os dias para alem das fronteiras geográficas, conhecimento é partilhado, e o mundo como o conhecemos é redesenhado a uma velocidade sem precedentes.

A segurança e a prosperidade de qualquer país depende cada vez mais na proteção das redes de TIC que gerem este crescimento de conhecimento e conexões, e é assim cada vez mais importante garantir no ciberespaço os direitos e deveres existentes na sociedade civil, na rede económica da sociedade e na comunidade internacional. A arena digital não é um espaço fora da lei, e é o nosso dever garantir que mesmo neste domínio os princípios democráticos e valores nos quais acreditamos são cumpridos, e as normas que preservam liberdades individuais, igualdade e liberdade, estão salva guardadas.

O ciberespaço chega a praticamente tudo e todos, fornece uma plataforma para a inovação e prosperidade, e os meios para melhorar o bem-estar geral a nível global. Mas com uma Infraestrutura digital com uma dimensão incalculável e pouco regulada, grandes riscos ameaçam nações, empresas privadas e direitos individuais. O governo tem a responsabilidade de agir nestas vulnerabilidades estratégicas para assegurar que Portugal e os seus cidadãos, juntos como comunidade, possam usufruir do potencial desta revolução das tecnologias da informação.

O governo não está organizado de um modo capaz de responder a este problema crescente de forma eficaz agora ou num futuro próximo. As responsabilidades dentro da cibersegurança são distribuídas pelas várias agências com as respetivas autoridade na matéria, por vezes sobrepondo-se umas as outras, e nenhuma com autoridade suficiente no processo de tomada de decisão para tomar ações diretas em muitos dos casos com que se deparam frequentemente.

8.1. O direito no ciberespaço e a regulamentação das ameaças virtuais

Os Ciberataques são cada vez mais comuns, capazes de desligar centrais nucleares, sistemas de defesa militares, redes elétricas, representam uma ameaça seria à segurança nacional. Como tal, alguns ataques podem até ser considerados atos de guerra. No entanto, estes ataques pouco ou nada se parecem com os ataques armados, não existem regras, e lei ainda é alheia a grande parte destas ameaças. Neste capítulo, vou apresentar uma breve reflexão sobre ciberataques e a falta de regulamentação que existe na lei relativamente a estes crimes e atos de guerra no ciberespaço.

Em 2010, o programa nuclear do Irão, alvo de um ataque sofisticado que fez com que as centrifugas perdessem o controlo, parando assim o projeto. A arma responsável por este ataque foi um "worm" [54], Conhecido como Stuxnet[55] que

[54] Worm- Um ***worm*** (termo da língua inglesa que significa, literalmente, "verme") é um programa autorreplicante, diferente de um vírus. Enquanto um vírus infecto um programa e necessita deste programa hospedeiro para se alastrar, o *worm* é um programa completo e não precisa de outro para se propagar. Um *worm* pode ser projetado para tomar ações maliciosas após infestar um sistema. Além de se auto replicar, pode deletar arquivos em um sistema ou enviar documentos por correio eletrónico.
[55] Stuxnet-**tuxnet** é um worm de computador projetado especificamente para atacar o sistema operacional SCADA (sistema desenvolvido pela Siemens para controlar as centrífugas de enriquecimento de urânio iranianas). Foi descoberto em junho de 2010 pela empresa bielorrussa desenvolvedora de antivírus VirusBlokAda. É o primeiro worm descoberto que espiona e reprograma sistemas industriais. Ele foi especificamente escrito para atacar o sistema de controlo industrial SCADA, usado para controlar e monitorar processos industriais. O Stuxnet é capaz de reprogramar CLPs e esconder as mudanças. O vírus

aparentemente tinha autores de várias partes do mundo e que foi provavelmente testado pelos Americanos e Israelitas.

Alguns meses depois, um ataque DDOs "distributed denial of service"[56] fez com que toda a população de Birmânia[57] ficasse sem internet pouco tempo antes das primeiras eleições do pais em vinte anos[58]. Alguns observadores suspeitam de que um grupo militar da Birmânia coordenou o ataque para desligar a internet e assim restringir a livre partilha de informação, mas oficiais americanos atribuem as culpas ao governo.

No verão de 2011, sugiram provas de um programa do governo chines, já há muito suspeito, um grupo militar chines que realizavam ataques DDOs ao *website* Falun Gong baseado em Alabama[59]. Esta revelação surgiu graças a um report feito pela empresa de cibersegurança McAfee no qual descreve um programa resultante de uma serie de ciberataques ao longo de vários anos que tinha como alvo uma variedade de governos como os Estados Unidos e vários países membros das Nações Unidas.[60]

---

pode estar camuflado em mais de 100 mil computadores, porém, para sistemas operacionais domésticos como o Windows e Mac OS X, o worm é inofensivo, só funciona efetivamente nas centrífugas de enriquecimento de urânio iranianas, já que cada usina possui sua própria configuração do sistema SCADA.

[56] DDOs – Um **ataque de negação de serviço** (também conhecido como DoS Attack, um acrônimo em inglês para *Denial of Service*), é uma tentativa de tornar os recursos de um sistema indisponíveis para os seus utilizadores. Alvos típicos são servidores web, e o ataque procura tornar as páginas hospedadas indisponíveis na WWW. Não se trata de uma invasão do sistema, mas sim da sua invalidação por sobrecarga.

[57] Birmânia -Myanmar ou Birmânia, oficialmente República da União de Myanmar (em birmanês), é um país do sul da Ásia continental limitado ao norte e nordeste pela China, a leste pelo Laos, a sudeste pela Tailândia, ao sul pelo Mar de Andamão e pelo Canal do Coco, a oeste pelo Golfo de Bengala e a noroeste pelo Bangladesh e pela Índia. Em 2006, a capital do país foi transferida de Rangum para Nepiedó.

[58] Burma Hit by Massive Net Attack Ahead of Election, BBCNEWS (Nov. 4, 2010, 3:33 PM), http://www.bbc.co.uk/news/technology-11693214.

[59] Ellen Nakashima & William Wan, China'sDenials on Cyberattacks Undercut, WASH.POST, Aug. 24, 2011, at A12.

[60] David Barboza & Kevin Drew, Security Firm Sees Global Cyberspying, N.Y.TIMES, Aug. 3, 2011, at A11. This was not the first suggestion of a program of cyber-attacks on private and government actors by China. Computer attacks on Google that originated in China were believed to be part of a broader political and corporate espionage effort and prompted Google to withdraw from the Chinese market. Ariana Eunjung Cha & Ellen Nakashima, GoogleAttack Part of Vast Campaign; Targets Are of Strategic Importance to China, Where Scheme Is Thought to Originate, WASH.POST,Jan. 14, 2010, at A1

Que leis regulam estes ataques? Existem algumas referências a este ataque e outros similares como "ciberguerra", sugerindo de que as leis de guerra se apliquem. No entanto, estes ataques em muito pouco se identificam com os tradicionais atos de guerra que estão regulados. Se estes atos são então considerados "atos de guerra", isso quer dizer que por exemplo no caso do Irão, este poderia responder legalmente com um ataque físico em resposta ao Stuxnet? Muitas destas e outras questões ainda estão por responder, a lei do ciberespaço ainda tem muito "buracos" para preencher. Numa realidade onde não se sabe quem é quem, nem de onde começa e acaba um ataque é difícil regular este tipo de ações.

Igualmente relevantes neste contexto de proteção do ciberespaço são, por um lado, o desenvolvimento da legislação como forma de prevenir e sancionar condutas consideradas lesivas para o desenvolvimento da sociedade da informação e do comércio eletrónico e, mais importante, perturbadoras do bom funcionamento de infraestruturas vitais para a sociedade, nomeadamente as infraestruturas críticas da informação e das comunicações, e, por outro, a eficaz repressão de atividades criminosas perpetradas contra ou p or intermédio das TIC.

Para atingir este objetivo são normalmente usadas duas vias distintas mas complementares: uma primeira visa a proteção do património e das pessoas através da criminalização dos ataques contra os sistemas informáticos e a informação neles contidos. Uma segunda via tem como objeto a regulamentação do mercado das telecomunicações e da indústria do TIC em geral, no sentido de assegurar um nível adequado de segurança para os seus utilizadores e para o Estado como um todo.

Tendo em consideração a escalada das várias formas de cibercrime aqui já brevemente enunciadas, na tentativa de limitar a sua expressão com base na repressão e dissuasão, um conjunto de organizações internacionais tem vindo a definir como prioridade para os seus Estados-membros a adaptação dos seus normativos legais e a capacitação das respetivas forças de segurança para fazer

face a esta nova realidade. Organizações internacionais como o Conselho da Europa (CoE),a União Europeia (UE), o Fórum Económico Ásia Pacífico (APEC), a Organização de Estados Americanos (OEA) e a OCDE criaram grupos de trabalho cuja principal missão consiste no desenvolvimento de iniciativas legislativas nesta área (Broadhurst and Chantler,2006). Entre estes destacam-se os trabalhos desenvolvidos no âmbito da ONU, do G8 e do CoE com a sua Convenção sobre o Cibercrime. A necessidade de produzir legislação específica para endereçar o problema do cibercrime foi primeiramente identificada no quinto Congresso das Nações Unidas de 1975 (Davin, 2004).[61] No entanto, só em 1990 a Assembleia Geral desta organização adotou uma resolução onde se identifica como necessário o desenvolvimento e formas e instrumentos de cooperação internacional para o combate ao cibercrime. Desta resolução resultou um manual sobre prevenção e controlo de crimes relacionados com computadores. Em 2000 a mesma Assembleia Geral adotou uma nova resolução em matéria de combate à utilização criminosa de tecnologias da informação, onde se reforça a necessidade de os Estados membros assegurarem que os seus regimes legais não resultem em verdadeiras zonas francas para o exercício de atividades criminosas desta natureza, mas também a inevitabilidade de uma maior cooperação na investigação criminal e judiciária transnacional. Ainda no plano da ONU, e do 11. Congresso sobre prevenção e justiça criminal, realizado em 2005, saiu uma declaração referindo a necessidade de harmonização legislativa no combate ao cibercrime.

O Conselho da União Europeia, p or seu lado, aprovou em 24 de Fevereiro de 2005, a Decisão-Quadro 2005/222/JAI relativa a ataques contra sistemas de informação. Esta tem por objetivo reforçar a cooperação entre as autoridades judiciárias e outras autoridades competentes dos Estados-membros mediante uma

[61] Resolução A/RES/45/121, Eighth United Nations Congress on the Presentation of Crime and the Treatment of Offfenders, disponível em http://www.un.org/documents/ga/res/45/a45r121.htm.

,

aproximação das suas disposições de direito penal em matéria de ataques contra os sistemas de informação.

Posto isto, serão suficientes estes esforços internacionais alicerçados em medidas punitivas e, portanto, dissuasoras, para prevenir e responder eficazmente a este tipo de ameaças à segurança nacional? Sem lhes retirar o destaque e o mérito que merecem porque necessários e mesmo essenciais, entendemos que não. Como referido no capítulo anterior, os desafios colo cados para proteger um país num cenário de ataque contra uma infraestrutura crítica vão muito além da perseguição das condutas desviantes individuais dentro do país ou além-fronteiras. Numa situação semelhante àquela vivida quer pela Estónia em 2007, quer pela Geórgia em 2008, tornou-se evidente a necessidade de os Estados possuírem instrumentos que permitam atuar junto dos operadores privados, nomeadamente tomarem medidas de prevenção, controlo e mitigação de incidentes. Por outras palavras, é necessário regular melhor o funcionamento do ciberespaço e tornar obrigatória, por via legislativa, a adoção de um conjunto mínimo de medidas de proteção e de capacidade de reação quer em redes públicas, quer privadas.

"Neste quadro, há a destacar o trabalho desenvolvido no seio da Comissão Europeia com vista à criação de um novo quadro regulatório para as comunicações eletrónicas, onde se pretende reforçar a responsabilidade dos operadores e o poder dos órgãos reguladores nacionais na supervisão da segurança das redes públicas de comunicações. Numa perspetiva de continuidade de negócio, este novo quadro regulatório vem reforçar a responsabilidade dos operadores de redes de comunicações públicas ou de serviços de comunicações eletrónicas acessíveis ao público, obrigando-os a realizar uma adequada gestão de riscos e a tomar as medidas necessárias para garantir a integridade das suas redes, de forma a impedir ou a minimizar o impacto de eventuais incidentes de segurança, assim como a responsabilidade de notificar a autoridade nacional de comunicações de eventuais violações de segurança ou de perda de integridade que tenha impacto significativo no funcionamento das redes e serviços." (José

Lino Santos, 2011). Por outro lado, o novo quadro vem reforçar, igualmente, a responsabilidade das autoridades nacionais de comunicações e os seus poderes junto dos operadores de redes de comunicações públicas ou de serviços de comunicações eletrónicas acessíveis ao público. Atribui aos primeiros o poder de emitir instruções vinculativas, de ordenar ou de realizar auditorias de segurança e de investigar os casos de incumprimento e os seus efeitos sobre a segurança e a integridade das redes e, aos segundos, de prestarem as informações necessárias para avaliar a segurança e/ou a integridade dos seus serviços e redes. Neste contexto, a ENISA desempenha um papel relevante de suporte à Comissão Europeia e aos Estados-membros. Na fase de discussão e transposição das diretivas, cabe à ENISA a articulação com as autoridades nacionais e com os operadores públicos de comunicações com vista à necessária harmonização de definições e do âmbito de aplicação do art.º 13 º A, introduzido pela Directiva 2009/140/CE, nomeadamente quanto às definições de violação de segurança e de perda de integridade, assim como à identificação do conjunto mínimo de medidas organizacionais e técnicas a exigir p elas autoridades reguladoras aos operadores públicos de comunicações. Neste novo quadro regulatório, cabe à ENISA o papel de aconselhamento à Comissão Europeia para emissão de novas medidas técnicas a respeitar pelos operadores. Para este efeito as autoridades reguladoras nacionais devem enviar à ENISA relatórios de incidentes e relatórios anuais de segurança.

Entidades Reguladoras

Quando se fala em direito e liberdades é necessário referir o maior órgão nacional fiscalizador de dados pessoais dos utilizadores portugueses para garantir de que os direitos e liberdades dos mesmos não estão a ser violados. A Comissão Nacional de Proteção de Dados (CNPD) é uma entidade administrativa independente com poderes de autoridade, que funciona junto da Assembleia da República. Tem como atribuição genérica controlar e fiscalizar o processamento de dados pessoais, em rigoroso respeito pelos direitos do homem e pelas liberdades e garantias consagradas na Constituição e na lei.
A Comissão é a Autoridade Nacional de Controlo de Dados Pessoais.
A CNPD coopera com as autoridades de controlo de proteção de dados de outros Estados, nomeadamente na defesa e no exercício dos direitos de pessoas residentes no estrangeiro.

À CNPD atribuem se as capacidades de maior relevância seguintes, controlar e fiscalizar o cumprimento das disposições legais e regulamentares em matéria de proteção de dados pessoais, exercer poderes de investigação e inquérito, podendo para tal aceder aos dados objeto de tratamento, exercer poderes de autoridade, designadamente o de ordenar o bloqueio, apagamento ou destruição dos dados, assim como o de proibir temporária ou definitivamente o tratamento de dados pessoais, Intervir em processos judiciais no caso de violação da lei de proteção de dados, intervir em processos judiciais no caso de violação da lei de proteção de dados e a responsabilidade de denunciar ao Ministério Público as infrações penais nesta matéria, bem como praticar os atos cautelares necessários e urgentes para assegurar os meios de provas.

Quanto às suas competências, a CNPD tem o poder de emitir pareceres sobre disposições legais e instrumentos jurídicos nacionais, comunitários e internacionais, relativos ao tratamento de dados pessoais, dar seguimento ao pedido efetuado por qualquer pessoa, ou por associação que a represente, para proteção dos seus direitos e liberdades, no que diz respeito ao tratamento de dados pessoais e informá-la do seu resultado, assegurar a representação junto de instâncias comuns de controlo de proteção de dados pessoais e exercer funções de representação e fiscalização no âmbito dos sistemas de Schengen e Europol tal como, emitir diretivas para sectores de atividade, relativas ao prazo de conservação dos dados, às medidas de segurança e aos códigos de conduta.

A Autoridade Nacional de Comunicações (ANACOM) tem por missão a regulação do sector das comunicações, incluindo as comunicações eletrónicas e postais e, sem prejuízo da sua natureza enquanto entidade administrativa independente, a coadjuvação ao Governo nestes domínios.

Estão atribuídas à ANACOM, ao abrigo dos seus estatutos e para o cumprimento da sua missão, enquanto autoridade reguladora nacional (ARN), atribuições como a gestão eficiente do espectro radioelétrico, envolvendo a planificação, a atribuição dos recursos espectrais, a sua supervisão e a coordenação entre as radiocomunicações civis, militares e paramilitares. A contribuição para o desenvolvimento do mercado interno das redes e serviços de comunicações eletrónicas e dos serviços postais da União Europeia (UE), e a aprovação do plano nacional de numeração (PNN), nomeadamente as suas linhas orientadoras e os seus princípios gerais, bem como assegurar a gestão eficiente dos recursos de numeração e endereçamento, incluindo a atribuição de recursos e definição de condições de utilização.

Em relação a entidades que prestam serviços de comunicações a ANACOM procede à resolução administrativa de litígios entre as entidades sujeitas à sua regulação, nomeadamente entre entidades que oferecem redes ou serviços de comunicações eletrónicas e entre prestadores de serviços postais, nos termos previstos na

legislação aplicável. A promoção á resolução extrajudicial de conflitos entre entidades sujeitas à sua regulação e os consumidores e demais utilizadores finais, em termos processuais simples, expeditos e tendencialmente gratuitos, dinamizando e cooperando com os mecanismos extrajudiciais de resolução de conflitos existentes ou, por sua iniciativa ou em colaboração com outras entidades, criando outros mecanismos, cabendo-lhe promover a adesão das entidades sujeitas à sua regulação. Num outro plano tem assegura a que seja mantido o acesso aos serviços de emergência a contribuição para garantir um elevado nível de proteção dos dados pessoais e da privacidade, e zelar pela manutenção da integridade e segurança das redes de comunicações públicas e dos serviços acessíveis ao público, incluindo as interligações nacionais e internacionais.

A nível organizacional no plano nacional a ANACOM tem no cumprimento da sua missão a atribuição de participar e, a pedido do Governo, assegurar a representação do Estado, em articulação com o Ministério dos Negócios Estrangeiros, em organismos e fóruns nacionais e internacionais com relevância para a respetiva atividade. Apoiar tecnicamente os organismos e serviços aos quais incumbe o acompanhamento do processo de estabelecimento e gestão da rede integrada de comunicações de emergência, assim como, contribuir para a definição e permanente atualização das políticas de planeamento civil de emergência no sector das comunicações.

Para além destas atribuições a ANACOM desempenha funções de entidade de supervisão central, com atribuições em todos os domínios regulamentados no Decreto-Lei n.º 7/2004, de 7 de janeiro[62]. Para prosseguir as suas atribuições, a ANACOM dispõe de poderes de regulamentação, supervisão, fiscalização e sancionatórios, cabendo-lhe nomeadamente, verificar o cumprimento das leis,

[62] Decreto-Lei n.º 7/2004, de 7 de janeiro- disciplina certos aspetos legais dos serviços da sociedade da informação, em especial do comércio eletrónico, em transposição da Diretiva 2000/31/CE, do Parlamento Europeu e do Conselho, de 8 de junho de 2000, salvo nas matérias em que lei especial atribua competência sectorial a outra entidade.

dos regulamentos e dos demais atos a que se encontram sujeitos os destinatários da sua atividade; verificar o cumprimento de qualquer orientação ou determinação por si emitida, ou de qualquer outra obrigação relacionada com o sector das comunicações; inspecionar, regularmente, os registos das queixas e reclamações dos consumidores e demais utilizadores finais apresentadas às entidades destinatárias da sua atividade, as quais devem preservar adequados registos das mesmas; praticar todos os atos necessários ao processamento e punição das infrações às leis e os regulamentos cuja implementação ou supervisão lhe compete, bem como as resultantes do incumprimento das suas determinações, incluindo, quando aplicável, adotar medidas cautelares, aplicar sanções, nomeadamente sanções pecuniárias compulsórias, e cobrar coimas.

Conclusão

Eventos passados vieram afirmar uma nova realidade, em 2016 a internet está presente no quotidiano de todos os cidadãos, empresas e organizações em todo o mundo, e estão interligadas entre si. Cenários como o da Estónia em 2007 vieram demonstrar que as ameaças são reais e o seu potencial, capazes de interromperem o funcionamento de um país. Como resposta a este cenário a Comissão Europeia (CE), em colaboração com a Alta Representante da União para os Negócios Estrangeiros e a Política de Segurança, publicou a 7 de fevereiro de 2013 a estratégia em matéria de cibersegurança e uma proposta de diretiva sobre a segurança das redes e da informação (SRI).

A estratégia em matéria de cibersegurança, denominada "Um ciberespaço aberto, seguro e protegido", traduz, segundo a CE, a visão global da União Europeia (UE) sobre a melhor forma de prevenir e dar resposta às perturbações e ataques na Internet. O objetivo da estratégia é constituir e financiar uma rede de centros

de excelência nacionais contra a cibercriminalidade para facilitar a formação e o desenvolvimento de capacidades no domínio da cibersegurança.

O plano de cibersegurança está assente em cinco prioridades:

(1). Alcançar a resiliência do ciberespaço;(2). Reduzir drasticamente a cibercriminalidade;(3). Desenvolver a política e as capacidades no domínio da ciberdefesa no quadro da política comum de segurança e defesa;(4). Desenvolver os recursos industriais e tecnológicos para a cibersegurança; (5). Estabelecer uma política internacional coerente em matéria de ciberespaço na Europa e promover os valores fundamentais da UE.

A CE publicou também uma proposta de diretiva sobre a segurança das redes e da informação (SRI), que considera ser uma componente fundamental na estratégia global de cibersegurança. A proposta requer que todos os Estados Membros, bem como os fornecedores de serviços de Internet e os operadores de infraestruturas garantam um ambiente digital seguro e fiável em toda a UE.

A diretiva proposta prevê, entre outras, as seguintes medidas:

Os Estados-Membros devem adotar uma estratégia em matéria de SRI e designar uma autoridade nacional competente para o sector, dotada dos recursos financeiros e humanos adequados para prevenir, gerir/tratar e dar resposta aos riscos e incidentes nesta área;

A criação de um mecanismo de cooperação entre os Estados-Membros e a CE que reúna, numa infraestrutura segura, os diferentes sistemas de alerta precoce para riscos e incidentes e facilite a colaboração e a organização de avaliações periódicas entre os pares;

Os operadores das infraestruturas críticas de alguns sectores (serviços financeiros, transportes, energia, saúde), os fornecedores de serviços da sociedade da informação (tais como lojas de aplicações online, plataformas de comércio eletrónico, pagamentos na Internet, computação em nuvem, motores de

pesquisa e redes sociais) e as administrações públicas devem adotar práticas de gestão do risco e notificar os incidentes de segurança graves ocorridos nos seus serviços essenciais.

Com estas iniciativas, a UE visa promover os valores europeus de liberdade e de democracia e garantir que a economia digital se desenvolve em condições de segurança.

A criação de infraestruturas para a proteção dos vários sectores não é suficiente para estarmos protegidos de todo o espectro de ciberameaças atual, é preciso desenvolver uma consciencialização aplicada ao cyber, capaz de detetar, perceber e responder a estas ameaças. Neste contexto surge o termo cyber situational awareness, que se apresenta como a consciência situacional no ciberespaço, ou seja, é através do cyber situational awareness que se pretende adquirir capacidades de prevenção e deteção necessárias para melhorar as capacidades defensivas de uma organização. Num nível mais avançado vimos também que o cyber situational awareness pode servir para prever futuros incidentes, oferecendo assim uma vantagem competitiva na resposta a incidentes.

Para se perceber causa e impacto destas ameaças, é preciso conhece-las, os seus comportamentos e intenções pois só assim podemos compreender o suficiente sobre a verdadeira natureza das ameaças que enfrentamos de modo a tomar as decisões acertadas para uma resposta eficaz. No estudo do cenário de ameaças deparamo-nos com vários termos, tais como ciberataque, e tentamos explorar a sua constituição, descobrindo assim que existe algo chamado, o ciclo de vida de um ciberataque, que nos demonstra que em cada ataque que ocorre existem um número de processos, que por norma, seguem um protocolo comum. Isto vai permitir assim atingir um conhecimento mais profundo do que são os ciberataques e como e quando devemos tomar medidas de mitigação para prevenir que este se propague até um ponto sem recuperação.

A maturidade de um centro de cibersegurança deve ser avaliada de tempo em tempo, sendo que esta é essencial para assegurar o bom funcionamento e a eficácia dos seus serviços. Um dos principais fatores de um modelo maturidade eficaz, é a sua capacidade de partilha de informação com outras entidades/organizações. Esta partilha de informação e crucial para o desenvolvimento das capacidades defensivas e para o aumento do nível de situational awareness como foi anteriormente referido. Considerando a partilha de informação, chegamos a conclusão de que existem atualmente uma variedade de arquiteturas de partilha de informação possíveis para implementar numa organização. A questão e adequar uma ou mais às necessidades existentes. Assim sendo percebemos que o mais importante é tirar o melhor proveito do conhecimento, experiencia, e das capacidades das outras organizações na partilha de informações sobre ameaças de modo a melhorarmos o nível de cibersegurança tanto da organização em causa como dos seus parceiros.

A internet como uma realidade presente no quotidiano de todos os cidadãos deve garantir a liberdades e direitos dos seus utilizadores. O ciberespaço não tem fronteiras e as suas capacidades não conhecem limites, como tal, a regulação deste espaço é um desafio atual. Já foram tomadas algumas medidas relativamente a regulamentações do ciberespaço, organizações internacionais já começaram a trabalhar em conjunto para desenvolverem normativas que se apliquem a nível internacional, mas nem sempre é fácil regular aquilo que não se conhece. A monotorização de sistemas, por exemplo, é uma ferramenta cada vez mais utilizada por organizações para detetar anomalias na rede, mas também utilizada por cibercriminosos em busca de vulnerabilidades nos sistemas para os poderem explorar para seu próprio benefício. Estas ferramentas tanto podem servir para garantir a segurança dos utilizadores tal como para lhes retirar aquilo que tentam proteger de início, a sua privacidade. É importante focarmo-nos no que importa, até que ponto deixamos de estar a garantir a segurança de uma pessoa ou organização e passamos a estar a invadir a sua privacidade ou integridade? São algumas destas questões em que nos devemos focar, e sem debilitar as capacidades das forças de segurança, conseguirmos regular e punir

aqueles que abusam destas ferramentas para beneficio pessoal. Sendo a internet um espaço livre, muitas destas ferramentas são facilmente acessíveis pelo utilizador comum, mas cabe às entidades fornecedoras a responsabilidade de restringir algumas ferramentas e às entidades reguladoras, a boa pratica das mesmas no ciberespaço.

Em suma, podemos afirmar que Portugal possui as capacidades necessárias para responder de forma eficaz às ciberameaças, mas com a evolução constante das mesmas é importante apostar no desenvolvimento e na formação. É necessário manter as infraestruturas atualizadas e os responsáveis pela segurança a par das ameaças emergentes. Como referido anteriormente é através da partilha de informação e articulação dos serviços, que se enriquece a base de dados de uma organização e se atingem os resultados esperados e o nível de maturidade pretendidos para garantir o nível de segurança desejado.

Portugal já possui um Centro Nacional de Cibersegurança, as infraestruturas estão estabelecidas, num mundo altamente interligado e interdependente, a segurança do ciberespaço requer uma forte cooperação e colaboração entre aliados e parceiros, nacionais e internacionais, alicerçada no desenvolvimento de confiança mútua, sendo preciso assim fortalecer a articulação entre as várias organizações nacionais e internacionais. O Centro Nacional de Cibersegurança tem como missão promover uma utilização consciente, livre, segura e eficiente do ciberespaço, valorizando os direitos e liberdades dos seus utilizadores e assegurar a segurança dos mesmos. É preciso afirmar o ciberespaço nacional como um domínio de desenvolvimento económico e de inovação.

No plano nacional, as estratégias estão delineadas e a missão definida, é preciso agora o desenvolvimento do modelo de maturidade, para que assim que atingir o nível desejado, o CNCS (Centro Nacional de Cibersegurança) possa ter ao seu dispor os meios e a capacidade necessária para a proteção eficaz do ciberespaço nacional.

Bibliografia

Chris Connolly, Alana Maurushat, David Vaile, Peter van Dijk, (2011) *An Overview of International Cyber-Security Awareness Raising and Educational Initiatives* ACMA – Australian Comunications and Media Authority;

Chris Johnson, Lee Badger, David Waltermire, (2014) *Guide to Cyber Threat Information Sharing* NIST Computer Security;

Carson Zimmerman, (2014) *Ten Strategies of a World-Class Cybersecurity Operations Center* The MITRE Corporation;

Amit P.Sheth, (2007) *Can Semantic Web Techniques Empower Comprehension and Projection in Cyber Situational Awareness?* The Ohio Center of Excellence in knowledge Enabled Computing;

Seclab, (2015) *A Cyber Awareness Framework for Attack Analysis, Prediction, and Visualization* https://seclab.cs.ucsb.edu/academic/projects/projects/cybaware/

Situational Awareness Reference Architecture (SARA), ICS-ISAC http://ics-isac.org/blog/sara/

John J. Salerno, Michael Hinman, and Douglas Boulware, *A Situation Awareness Model Applied to Multiple Domains. Proceedings of the Defense and Security Conference,* Orlando FL, (March 2005);

Mica R. Endsley, *Toward a Theory of Situation Awareness in Dynamic Systems. Human Factors Journal,* Volume 37 (1), pages 32-64, March 1995;

John J. Salerno, et al., *Achieving Situation Awareness in a Cyber Environment. Proceedings of the Situation Management Workshop* of MILCOM 2005, Atlantic City NJ, (October 2005);

George Tadda, et al., *Realizing Situation Awareness within a Cyber Environment. In Multisensor, Multisource Information Fusion: Architectures, Algorithms, and Applications* (2006), edited by Belur V. Dasarathy, Proceedings of

SPIE Vol. 6242 (SPIE, Bellingham, WA, 2006) 624204, Kissimmee FL, April 2006;

José Lino Alves dos Santos, 2011 "Contributos para uma melhor governação da cibersegurança em Portugal"

Shawn Riley, *Insights to Modern Cyber Threat Intelligence*, (fev. 2015) https://www.linkedin.com/pulse/insights-modern-cyber-threat-intelligence-shawn-riley

Walter Cooke, *Situation Awareness & Cyber Security Defense*, (fev. 2015), CISSP https://www.linkedin.com/pulse/situation-awareness-cyber-security-defence-walter-cooke-cissp

*Continuous Cyber Situational Awareness***,** *Continuous monitoring of security controls and comprehensive cyber situational awareness represent the building blocks of proactive network security.* (2014), Lumeta Corporation

Cyber Situational Awareness: The Ability to Make Informed Risk Management Decisions (October. 2012)

P. Barford, M. Dacier, T. G. Dietterich, M. Fredrikson, J. Giffin, S. Jajodia, S. Jha, J. Li, P. Liu, P. Ning, X. Ou, D. Song, L. Strater, V. Swarup, G. Tadda, C. Wang, and J. Yen, *Cyber SA: Situational Awareness for Cyber Defense*, (2009), *capitulo nº1, pág. (3-14)*

Noluxolo Kortjan, Rossouw von Solms, *A conceptual framework for cyber-security awareness and education in SA,* (2014) School of ICT, Nelson Mandela Metropolitan University, South Africa, pág. (29-40)

Ulrik Franke, Joel Brynielsson, *Cyber situational awareness - A systematic review of the literature*, (2014), FOI Swedish Defence Research Agency, *pág. (18-31)*

Judson Dressler, William Moody, Calvert L.bowen, III, Jason Koepke, *Operational Data Classes for Establishing Situational Awareness in Cyberspace*, (2014) 6th International Conference on Cyber Conflict, NATO CCD COE Publications, Tallinn

Joel Brynielsson, *A Gaming Perspective on Comand and Control*, (2006) pág. (17-19) pdf

Internet Governance Forum (IGF) 2014, *Best Practice Forum on Establishing and Supporting Computer Security Incident Response Teams (CSIRT) for Internet Security pág. (1-20)*

CCDCOE, *Nato Cyber Security Strategy Documents (2015) https://ccdcoe.org/strategies-policies.html*

Matt Hartley, *THREAT INTELLIGENCE http://www.darkreading.com/analytics/threat-intelligence/cyber-threats-information-vs-intelligence/a/d-id/1316851*

Situation Awareness (SA) (2006) COPYRIGHT SPIE--The International Society for Optical Engineering

Ulrik Franke, Joel Brynielsson, *Computers & Security* FOI Swedish Defence Research Agency Stockholm, Sweden

Endsley, M. R., & Garland, D. J. (Eds.). (2000). *Situation awareness analysis and measurement*. Mahwah, NJ: Lawrence Erlbaum Associates.

Endsley, M. R. (2004). *Situation awareness: Progress and directions*. In Banbury, S., & Tremblay, S. (Eds.), *A cognitive approach to situation awareness: Theory, measurement and application* (pp. 317 – 341). Aldershot, UK: Ashgate Publishing

MATHEW VARGHESE *Actionable CTI* https://www.linkedin.com/pulse/rise-stand-alone-cyber-threat-intelligence-cti-mathew-varghese The Rise of "Stand-alone" *Cyber Threat Intelligence (CTI)* (2014)

Broadhurst, R. (2006). Developments in the global law enforcement of cyber-crime.Policing An International Journal of Police Strategies Management 29 (3), pp. 408-433.